

PBW bases for a class of braided Hopf algebras [★]

Stefan Ufer ¹

*Mathematisches Institut der Universität München, Theresienstr. 39,
80333 München, Germany*

Abstract

We prove the existence of a basis of Poincaré-Birkhoff-Witt type for braided Hopf algebras R generated by a braided subspace $V \subset P(R)$ if the braiding on V fulfils a triangularity condition. We apply our result to pointed Hopf algebras with abelian coradical and to Nichols algebras of low dimensional simple $U_q(\mathfrak{sl}_2)$ -modules.

1 Introduction

This paper deals with two concepts from combinatorial algebra. The first is the concept of PBW bases. It is a well known classical result from the theory of Lie algebras that the universal enveloping algebra of a Lie algebra has a basis of elements of the form

$$x_1^{e_1} \cdot \dots \cdot x_n^{e_n}$$

with $n \in \mathbb{N}_0$, $e_1, \dots, e_n \in \mathbb{N}_0$ and $x_1 > \dots > x_n$ elements of a totally ordered basis of the Lie algebra. This theorem is due to Poincaré, Birkhoff and Witt and the basis is called the PBW basis of the universal enveloping algebra. We say that the basis of the Lie algebra generates the PBW basis of the enveloping algebra. We give a formalization of this concept in definition 32, incorporating also the analog basis for universal enveloping algebras of p -Lie algebras. In [1] Kharchenko proves that such a basis exists for a much larger class of Hopf algebras. Based on his ideas our main theorem proves the existence of a PBW

[★] This work will be part of the authors PhD thesis written under the supervision of Professor H.-J. Schneider.

¹ Partially supported by Graduiertenförderung des bayerischen Staates and by his parents

basis for a large class of braided Hopf algebras.

The other concept is the concept of Lyndon words. These are those words in letters from a set X that are lexicographically smaller than any of their ends (see definition 11). These words are in bijection with a basis of the free Lie algebra over the set X [2]. This bijection offers a close connection between a PBW basis of the enveloping algebra of a Lie algebra \mathfrak{g} generated by some set X (and various relations) and the set of Lyndon words with letters from the set X . As the elements generating the PBW basis are iterated Lie brackets in elements from X they can be described as iterated commutators of elements of X in the enveloping algebra [3]. This correspondence is a very special case of the central theorem in [1] and in this paper.

More recent results first found by Lusztig [4,5] and Rosso [6,7], then also by Ringel [8] showed that also the deformed enveloping algebras of finite dimensional semisimple complex Lie algebras introduced by Drinfel'd [9,10] and Jimbo [11] have a PBW basis in the sense of definition 32. Later Leclerc observed that the connection to the theory of Lyndon words is preserved under this deformation [12]. He gives an algorithm to compute the generating set for a PBW basis of the positive part $U_q^+(\mathfrak{g})$ in terms of Lyndon words.

For general (graded) algebras it is an interesting question whether they admit a (non-trivial) PBW basis or not. The results in the setting of quantum groups treated by now are quite concrete, which is mostly due to the existence of a braid group action [5]. In [1] Kharchenko follows a more combinatoric approach not relying on a root system or a braid group action. He finds a PBW basis for Hopf algebras generated by an abelian group and a finite set of skew primitive elements such that the adjoint action of the group on the skew primitive generators is given by multiplication with a character. This result can be reinterpreted to provide a PBW basis for braided Hopf algebras in the category of Yetter-Drinfel'd modules over an abelian group which are generated by a completely reducible Yetter-Drinfel'd submodule of primitive elements. In contrast to the results on quantum groups that do only apply to special quotients of the braided tensor algebra, namely the Nichols algebras, Kharchenko's result covers arbitrary braided bialgebra quotients of the tensor algebra.

It is a priori not clear, if such a strong result generalizes to other situations. In this paper we give a generalization of Kharchenko's result to a bigger family of braided Hopf algebras. The assumption that the braiding on the set of primitive generators is diagonal is replaced by a more general assumption of triangularity (definition 15). The main theorem of this paper says that every braided bialgebra quotient of the tensor algebra of a triangular braided vector space admits a PBW basis.

For our combinatorial proof triangularity of the braiding seems to be the natural setting. This situation includes for example a class of braided Hopf algebras constructed from representations of $U_q(\mathfrak{g})$ for \mathfrak{g} a finite dimensional semisimple complex Lie algebra or a Kac-Moody Lie algebra. Remark 17 offers

a more conceptual characterization of triangular braidings.

Following a suggestion of the referee we apply this theorem to generalize Kharchenko's existence result for the PBW basis in the sense that the action of the group on the space of skew primitive elements is not required to be via characters any more.

The approach we take to prove the central theorem is a generalization of Kharchenko's proof and makes intensive use of the comultiplication available in the braided Hopf algebra. The lack of the braid group action is paid for by a less concrete result. In general the bases given by Kharchenko and in this paper can not be computed without knowledge of the relations in the braided Hopf algebra. However also in the step from diagonal to triangular braidings we lose some information (see remark 36). Nevertheless some results obtained for Nichols algebras of simple $U_q(\mathfrak{sl}_2)$ modules are treated in the last section. They contribute to answering a question raised by N. Andruskiewitsch in [13].

The paper is organized as follows: Section 2 is devoted to the definition and general facts on braided bialgebras. In particular we discuss the Nichols algebra of a braided vector space. Section 3 provides basic facts about Lyndon words. For proofs of the results in this section the reader is referred to the literature [14,2,15]. In Section 4 the setting for the central theorem - braidings of left (resp. right) triangular type - are introduced. We study braided commutators in the tensor algebra of the braided vector space. These will be a major tool for the proof of the main theorem. Section 5 deals with technical combinatorial facts about the comultiplication in the tensor algebra of a left triangular braided vector space. These results rely heavily on the condition of triangularity. In section 6 we define the data describing the PBW basis for any braided bialgebra quotient of the tensor algebra and prove the main theorem. Furthermore we prove a result providing an important restriction on the heights of the PBW generators. Section 7 offers a transfer of the results to right (instead of left) triangular braidings. Section 8 contains the application of our result to Hopf algebras generated by an abelian group and finitely many skew primitive elements. Finally in section 9 we study Nichols algebras of simple $U_q(\mathfrak{sl}_2)$ modules of low dimension.

Throughout the paper k will be a field, all vector spaces will be k -vector spaces and all tensor products are taken over k .

I would like to thank the referee for useful comments, my supervisor Prof. Schneider for his guidance and István Heckenberger for helpful discussions.

2 Braided vector spaces and braided bialgebras

In this section we review some basic facts about braided Hopf algebras.

Definition 1 *A braided vector space is a vector space V together with an automorphism c of $V \otimes V$ that satisfies the braid equation:*

$$(c \otimes \text{id}_V)(\text{id}_V \otimes c)(c \otimes \text{id}_V) = (\text{id}_V \otimes c)(c \otimes \text{id}_V)(c \otimes \text{id}_V).$$

We define further isomorphisms

$$c_{n,m} : V^{\otimes n} \otimes V^{\otimes m} \rightarrow V^{\otimes m} \otimes V^{\otimes n} \text{ for } m, n \geq 0$$

inductively by $c_{0,1} = \text{id}_V$, $c_{1,0} = \text{id}_V$, $c_{0,0} = \text{id}_k$, $c_{1,1} = c$ and

$$c_{1,m+1} = (\text{id}_V \otimes c_{1,m})(c \otimes \text{id}_{V^{\otimes m}}), c_{n+1,m} = (c_{n,m} \otimes \text{id}_V)(\text{id}_{V^{\otimes n}} \otimes c_{1,m}).$$

This induces an automorphism $\hat{c} : T(V) \otimes T(V) \rightarrow T(V) \otimes T(V)$ turning the tensor algebra $T(V)$ of V into a braided vector space $(T(V), \hat{c})$. From now on we will denote the braiding on $T(V)$ by c as well.

If (V, c) is a braided vector space and $f : V^{\otimes n} \rightarrow V^{\otimes m}$ is a homomorphism we say that f commutes with c if

$$(f \otimes \text{id}_V)c_{1,n} = c_{1,m}(\text{id}_V \otimes f) \text{ and } (\text{id}_V \otimes f)c_{n,1} = c_{m,1}(f \otimes \text{id}_V).$$

The braid equation says that c commutes with c .

Assume A is an algebra and (A, c) a braided vector space such that the product $m : A \otimes A \rightarrow A$ and the unit $\eta : A \rightarrow k$ of A commute with c . Define $A \underline{\otimes} A := A \otimes A$ as a vector space. Endowed with the maps

$$\begin{aligned} m_{A \underline{\otimes} A} &:= (m_A \otimes m_A)(\text{id}_A \otimes c \otimes \text{id}_A) : (A \underline{\otimes} A) \otimes (A \underline{\otimes} A) \rightarrow A \underline{\otimes} A, \\ \eta_{A \underline{\otimes} A} &:= \eta_A \otimes \eta_A : k \rightarrow A \underline{\otimes} A. \end{aligned}$$

this is an algebra. Furthermore the opposite algebra $A^{op,c}$ is the algebra obtained from A using the multiplication $m_{A^{op,c}} = m_A c$.

Dually, if C is a coalgebra and (C, c) is a braided vector space such that Δ, ε commute with c , define $C \underline{\otimes} C := C \otimes C$ as a vector space. Endowed with the maps

$$\begin{aligned} \Delta_{C \underline{\otimes} C} &:= (\text{id}_C \otimes c \otimes \text{id}_C)(\Delta_C \otimes \Delta_C) : C \underline{\otimes} C \rightarrow (C \underline{\otimes} C) \otimes (C \underline{\otimes} C), \\ \varepsilon_{C \underline{\otimes} C} &:= \varepsilon_C \otimes \varepsilon_C : C \underline{\otimes} C \rightarrow k. \end{aligned}$$

this is a coalgebra. The following definition of a braided Hopf algebra is equivalent to that of [16].

Definition 2 A braided bialgebra (R, c) (or R) is a tuple $(R, m, \eta, \Delta, \varepsilon, c)$ such that

- (R, m, η) is an algebra,
- (R, Δ, ε) is a coalgebra,
- (R, c) is a braided vector space,
- $m, \eta, \Delta, \varepsilon$ commute with c

and one of the two following equivalent conditions holds:

- $\Delta : R \rightarrow R \otimes R$ and $\varepsilon : R \rightarrow k$ are algebra homomorphisms.
- $m : R \otimes R \rightarrow R$ and $\eta : k \rightarrow R$ are coalgebra homomorphisms.

A homomorphism $f : (R, c) \rightarrow (R', d)$ of braided bialgebras is a homomorphism of algebras and coalgebras such that $(f \otimes f)c = d(f \otimes f)$.

As usual $\text{Hom}_k(R, R)$ is an algebra with the convolution product and R is called a braided Hopf algebra if the identity on R is convolution invertible. In this case the convolution inverse of the identity is called the antipode of R .

An element $x \in R$ is called primitive if we have $\Delta(x) = 1 \otimes x + x \otimes 1$. Let $P(R) := \{x \in R | x \text{ primitive}\}$.

If (R, c) is a braided Hopf algebra, the antipode commutes with the braiding [16].

Remark 3 Let H be a Hopf algebra with bijective antipode. Every bialgebra (Hopf algebra) in the category of Yetter-Drinfel'd modules over H is a braided bialgebra (braided Hopf algebra) in the sense of this definition. Conversely Takeuchi shows that every rigid braided bialgebra (Hopf algebra) can be realized as a bialgebra (Hopf algebra) in the category of Yetter-Drinfel'd modules over some Hopf algebra with bijective antipode [16].

Nevertheless our notion of a morphism of braided bialgebras is weaker than that of a morphism of bialgebras in a Yetter-Drinfel'd category. Assume that we have a bialgebra R in the category of Yetter-Drinfel'd modules over some Hopf algebra. A subbialgebra R' in this setting is a Yetter-Drinfel'd submodule and thus we have automatically induced braidings

$$R' \otimes R \rightarrow R \otimes R', R' \otimes R \rightarrow R \otimes R' \text{ and } R' \otimes R' \rightarrow R' \otimes R'.$$

On the other hand assume we have a braided bialgebra R'' that is a braided subbialgebra of R in the sense that the inclusion is a morphism of braided bialgebras, but R'' is not necessarily a Yetter-Drinfel'd submodule. In this case we obtain only a braiding for R''

$$R'' \otimes R'' \rightarrow R'' \otimes R''.$$

In [16] R'' is called a *non-categorical* (braided) subbialgebra of R in this case.

Lemma 4 *Let (V, c) be a braided vector space. Then the tensor algebra $T(V)$ admits a unique structure of a braided Hopf algebra such that the elements of V are primitive.*

PROOF. Define Δ , ε and $S : T(V) \rightarrow T(V)^{op, c}$ using the universal property of the tensor algebra such that for all $v \in V$ we have $\Delta(v) = 1 \underline{\otimes} v + v \underline{\otimes} 1$, $\varepsilon(v) = 0$, $S(v) = -v$. So Δ and ε are algebra homomorphisms. It is easy to check that the set of elements $x \in T(V)$ satisfying $(\text{id} \star S)(x) = \varepsilon(x)$ and $(S \star \text{id})(x) = \varepsilon(x)$ is closed under multiplication. Checking this equation for the generators is trivial, so S is a convolution inverse of id . Of course ε commutes with c . By the construction, Δ is a composition of homomorphisms of the type $V^{\otimes i} \otimes c \otimes V^{\otimes j}$, $i, j \geq 0$ (for exact formulas see [17]). As c commutes with c , these homomorphisms commute with c and so does Δ . \square

Remark 5 If (R, c_R) is a braided bialgebra and $V := P(R)$ its space of all primitive elements, we have

$$c_R(V \otimes V) \subset V \otimes V.$$

Lemma 6 *Let (R, c_R) be a braided bialgebra, $V \subset P(R)$ a braided subspace (this means $c_R(V \otimes V) = V \otimes V$). Then there is a unique homomorphism of braided bialgebras $\pi : T(V, c_R|_{V \otimes V}) \rightarrow R$ with $\pi|_V = \text{id}_V$.*

PROOF. Uniqueness is obvious. Of course π exists as algebra homomorphism. Denote the braiding on the tensor algebra induced by $c_R|_{V \otimes V}$ by $c_{T(V)}$. Using the universal property of the tensor algebra we obtain that π is a coalgebra homomorphism, provided $\pi \otimes \pi : T(V) \underline{\otimes} T(V) \rightarrow R \underline{\otimes} R$ is an algebra homomorphism. It is easy to check this, if $(\pi \otimes \pi)c_{T(V)} = c_R(\pi \otimes \pi)$. So we are left to show this. By construction we have $\pi|_{V^{\otimes l}} = m_l|_{V^{\otimes l}}$, a restriction of the l -fold multiplication of R . Thus for all $r, s \geq 0$

$$\begin{aligned} (\pi \otimes \pi)c_{T(V)}|_{V^{\otimes r} \otimes V^{\otimes s}} &= (m_s \otimes m_r)(c_{T(V)})_{r,s}|_{V^{\otimes r} \otimes V^{\otimes s}} \\ &= c_R(m_r \otimes m_s)|_{V^{\otimes r} \otimes V^{\otimes s}} \\ &= c_R(\pi \otimes \pi)|_{V^{\otimes r} \otimes V^{\otimes s}}, \end{aligned}$$

where the second equality is because the multiplication of R commutes with c . \square

Definition 7 *Let (R, c) be a braided bialgebra. A subspace $I \subset R$ is called a (braided) biideal, if it is an ideal, a coideal and*

$$c(R \otimes I + I \otimes R) = R \otimes I + I \otimes R.$$

If (R, c) is a braided Hopf algebra with antipode S , I is called a (braided) Hopf ideal if it is a biideal with $S(I) \subset I$.

Lemma 8 *Let (R, c) be a braided bialgebra.*

- (1) *If $I \subset R$ is a braided biideal there is a unique structure of a braided bialgebra on the quotient R/I such that the canonical map is a homomorphism of braided bialgebras.*
- (2) *If $\pi : (R, c) \rightarrow (S, d)$ is a morphism of braided bialgebras, $\ker \pi$ is a braided biideal of R .*
- (3) *Analogous statements hold for braided Hopf ideals.*

PROOF. Part 1: Uniqueness is clear because π is surjective. Obviously R/I is an algebra and a coalgebra in the usual way with structure maps $\bar{m}, \bar{\eta}, \bar{\Delta}$ and $\bar{\varepsilon}$. Furthermore $c(\ker(\pi \otimes \pi)) = \ker(\pi \otimes \pi)$ and thus c induces an automorphism \bar{c} of $R/I \otimes R/I$ such that $(\pi \otimes \pi)c = \bar{c}(\pi \otimes \pi)$. Surjectivity of $\pi \otimes \pi$ ensures that \bar{c} satisfies the braid equation and that $\bar{\Delta}, \bar{\varepsilon}$ are algebra homomorphisms. $\bar{m}, \bar{\eta}, \bar{\Delta}, \bar{\varepsilon}$ commute with \bar{c} because $m, \eta, \Delta, \varepsilon$ commute with c and π is surjective.

Part 2: Of course $I := \ker \pi$ is an ideal and a coideal. It remains to show that the condition for c holds. As $(\pi \otimes \pi)c = d(\pi \otimes \pi)$ and c is bijective we have $c(\ker(\pi \otimes \pi)) = \ker(\pi \otimes \pi)$. In view of $\ker(\pi \otimes \pi) = I \otimes R + R \otimes I$ the proof is complete. \square

Example 9 *The Nichols algebra of a braided vector space.* Let (V, c) be a braided vector space. The Nichols algebra $\mathcal{B}(V, c)$ as defined in [18] satisfies

- $\mathcal{B}(V, c) = \bigoplus_{n \in \mathbb{N}_0} R(n)$ is a graded braided Hopf algebra (this means graded as algebra, coalgebra and braided vectorspace simultaneously),
- $R(0) \simeq k$ and $R(1) \simeq V$ as braided vector spaces,
- $R(1) = P(R)$ and
- R is generated by $R(1)$ as an algebra.

The Nichols algebra for a braided vector space (V, c) exists and is unique up to isomorphism. It is a braided analogue of the classical symmetric algebra. See [17, 18] for more details.

3 Lyndon words

The PBW basis constructed later is closely related to Lyndon words in letters from a set X of primitive elements of the braided bialgebra. In this section we discuss the necessary facts about Lyndon words. Let $(X, <)$ be a finite

totally ordered set and \mathbb{X} the set of all words in the letters X (the free monoid over X). Throughout this section all words will be from \mathbb{X} . Recall that the *lexicographical order* on \mathbb{X} is the total order defined in the following way: For words $u, v \in \mathbb{X}$, $u < v$ iff either $v \in u\mathbb{X}$ (u is the beginning of v) or if there exist $r, s, t \in \mathbb{X}, a, b \in X$ such that

$$u = ras, v = rbt \text{ and } a < b.$$

For example if $x, y \in X, x < y$ then $x < xy < y$.

Notation 10 For a word $u \in \mathbb{X}$ let $l(u)$ be the length of u . Define $\mathbb{X}^n := \{u \in \mathbb{X} | l(u) = n\}$, for $v \in \mathbb{X}$ let $\mathbb{X}_{>v} := \{u \in \mathbb{X} | u > v\}$, $\mathbb{X}_{\geq v} := \{u \in \mathbb{X} | u \geq v\}$, $\mathbb{X}_{>v}^n := \mathbb{X}^n \cap \mathbb{X}_{>v}$ and $\mathbb{X}_{\geq v}^n := \mathbb{X}^n \cap \mathbb{X}_{\geq v}$.

Definition 11 Let $u \in \mathbb{X}$. The word u is called a *Lyndon word* if $u \neq 1$ and u is smaller than any of its proper endings. This means for all $v, w \in \mathbb{X} \setminus \{1\}$ such that $u = vw$ we have $u < w$.

These words are also called *regular words* in [15] or *standard words* in [1].

A word u is Lyndon if and only if for every factorization $u = vw$ of u into nonempty words v, w we have $u < vw$ ([14], 5.1.2.)

Theorem 12 (Lyndon, see [14], theorem 5.1.5.)

Any word $u \in \mathbb{X}$ may be written uniquely as a nonincreasing product of Lyndon words

$$u = l_1 l_2 \dots l_r, \quad l_i \text{ Lyndon words and } l_1 \geq l_2 \geq \dots \geq l_r.$$

This decomposition is obtained inductively by choosing l_1 to be the longest beginning of u that is a Lyndon word. It will be referred to as the *Lyndon decomposition* of u . The occurring Lyndon words are called the *Lyndon letters* of u .

Theorem 13 ([2], theorem 5.1. and section 4.1.)

The set of Lyndon words is a Hall set with respect to the lexicographical order. This means that for every Lyndon word $u \in \mathbb{X} \setminus X$ we have a fixed decomposition $u = u'u''$ into nonempty Lyndon words u', u'' such that either $u' \in X$ or the decomposition of u' has the form $u' = vw$ with $w \geq u''$.

This decomposition is obtained by choosing u'' to be the minimal (with respect to the lexicographical order) or (equivalently) the longest end of u that is Lyndon. As in [1] it is referred to as the *Shirshov decomposition* of u .

Lemma 14 ([1], Lemma 5)

For $u, v \in \mathbb{X}$ we have $u < v$ if and only if u is smaller than v when comparing them using the lexicographical order on the Lyndon letters. This means if $v = l_1 \dots l_r$ is the Lyndon decomposition of v , we have $u < v$ iff

- u has Lyndon decomposition $u = l_1 \dots l_i$ for some $0 \leq i < r$
- or u has Lyndon decomposition $u = l_1 \dots l_{i-1} \cdot l \cdot l'_{i+1} \dots l'_s$ for some $1 \leq i < r, s \in \mathbb{N}$ and some Lyndon words l, l'_{i+1}, \dots, l'_s with $l < l_i$.

4 Braided commutators in the tensor algebra

Major tools for constructing the PBW Basis will be the braided commutators discussed in this section. Take a finite dimensional vectorspace V , an endomorphism r of $V \otimes V$ satisfying the braid equation and a basis X of V . Define the endomorphism $r_{n,m} : V^{\otimes n} \otimes V^{\otimes m} \rightarrow V^{\otimes m} \otimes V^{\otimes n}$ in the same way as for braidings. We will omit the indices n, m whenever it is clear from the context which endomorphism is used.

Identify $k\mathbb{X}$ - the free algebra over X - with the tensor algebra of V in the obvious way and construct a k -linear endomorphism $[-]_r$ of $k\mathbb{X}$ inductively. Set for all $x \in X$

$$[1]_r := 1 \quad \text{and} \quad [x]_r := x.$$

For Lyndon words $u \in \mathbb{X}$ of degree > 1 with Shirshov decomposition $u = vw$ define

$$[u]_r := m(\text{id} - r_{l(v), l(w)})([v]_r \otimes [w]_r),$$

where m denotes multiplication in $k\mathbb{X}$. For arbitrary words with Lyndon decomposition $u = u_1 \dots u_t$ let

$$[u]_r := [u_1]_r \dots [u_t]_r.$$

Obviously $[-]_r$ is a graded homomorphism of the graded vectorspace $k\mathbb{X}$. The idea of using a homomorphism of this type to construct PBW bases can be found in [1] and is motivated by the theory of (free) Lie algebras.

For the rest of this paper we will only deal with braidings that fulfil a certain combinatorical condition.

Definition 15 *Let V be a finite dimensional vector space with a totally ordered basis X and $c \in \text{End}(V \otimes V)$.*

The endomorphism c will be called left triangular (with respect to the basis X) if for all $x, y, z \in k$ with $z > y$ there exist $\gamma_{x,y} \in k$ and $v_{x,y,z} \in V$ such that for all $x, y \in X$

$$c(x \otimes y) = \gamma_{x,y} y \otimes x + \sum_{z > y} z \otimes v_{x,y,z}.$$

The endomorphism c will be called right triangular (with respect to the basis X) if for all $x, y, z \in k$ with $z > y$ there exist $\beta_{x,y} \in k$ and $w_{x,y,z} \in V$ such that for all $x, y \in X$

$$c(x \otimes y) = \beta_{x,y} y \otimes x + \sum_{z > x} w_{x,y,z} \otimes z.$$

A braided vector space (V, c) will be called left (resp. right) triangular with respect to the basis X if c is left (resp. right) triangular with respect to the basis X .

Remark 16 The name "left triangular" is motivated by the following observation: Assume in the situation of the definition that V has dimension n and denote by $B = (b_1, \dots, b_{n^2})$ the basis $\{x \otimes y | x, y \in X\}$ of $V \otimes V$ ordered lexicographically. By $B^{op} = (b'_1, \dots, b'_{n^2})$ denote the basis obtained from B by flipping the sides of every tensor (not changing the order). Then the matrix $A \in \text{GL}(n^2, k)$ satisfying $c(b'_1, \dots, b'_{n^2}) = (b_1, \dots, b_{n^2})A$ has the following form:

$$A = \begin{pmatrix} D_1 & 0 & \dots & 0 \\ \star & D_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ \star & \dots & \star & D_n \end{pmatrix},$$

where $D_1, \dots, D_n \in \text{GL}(n, k)$ are diagonal matrices. If the braiding was diagonal (defined after the next example), this matrix would be diagonal.

Remark 17 In [19] we show that for a braided vectorspace (V, c) the following statements are equivalent:

- c is right triangular
- There is a pointed Hopf algebra H with abelian coradical having M as a (left-left) Yetter-Drinfel'd module such that the induced braiding is c and $G(H)$ acts diagonally on M .

For technical reasons we will first deal with left triangular braidings. In section 7 we will transfer our results to the right triangular case.

Example 18 Assume $k = \mathbb{C}$. Let \mathfrak{g} be a finite dimensional semisimple complex Lie algebra and $q \in \mathbb{C}$ not a root of unity. Let $\Phi \subset V$ be the root system of \mathfrak{g} (V a finite dimensional \mathbb{Q} vector space), fix a basis $\Pi = \{\mu_1, \dots, \mu_s\}$ of it and denote by $\Lambda \subset V$ the weight lattice. For any finite dimensional $U_q(\mathfrak{g})$ -module M of type 1 with weight space decomposition $M = \bigoplus_{\mu \in \Lambda} M_\mu$ we have a $U_q(\mathfrak{g})$ linear braiding (see [20], Chapter 7)

$$\Theta : M \otimes M \rightarrow M \otimes M.$$

This braiding is built up of \mathbb{C} -linear maps

$$\Theta_\nu : M \otimes M \rightarrow M \otimes M \text{ for } \nu \in \mathbb{Z}\Phi, \nu \geq 0$$

satisfying for all $\mu, \mu' \in \Lambda, \nu \in \mathbb{Z}\Phi, \nu \geq 0$

$$\Theta_\nu(M_\mu \otimes M_{\mu'}) \subset M_{\mu' - \nu} \otimes M_{\mu + \nu}$$

and a map

$$f : \Lambda \times \Lambda \rightarrow \mathbb{C}$$

in the following way: For $a \in M_\mu, b \in M_{\mu'}$ we have

$$\Theta(a \otimes b) = f(\mu', \mu) \sum_{\nu \geq 0} \Theta_\nu(b \otimes a).$$

Note that the sum is actually finite because for finite dimensional modules M only finitely many weight spaces M_μ can be different from zero. We will construct a basis B of M such that the braiding Θ is left triangular with respect to this basis.

Now consider the total order \triangleright defined on V using the basis Π in the following way:

$$\sum_{i=1}^s a_i \mu_i \triangleright \sum_{i=1}^s b_i \mu_i \Leftrightarrow (a_1, \dots, a_s) > (b_1, \dots, b_s),$$

where on the right side we order the sequences in \mathbb{Q}^s lexicographically by identifying them with words of s letters from \mathbb{Q} .

Then for $\mu, \mu', \nu \in V$ $\mu \triangleright \mu'$ implies $\mu + \nu \triangleright \mu' + \nu$ and $\nu > 0$ implies $\nu \triangleright 0$. For every $\mu \in \Lambda$ with $M_\mu \neq 0$ choose a totally ordered basis (B_μ, \leq) of M_μ and order the union $B = \cup_\mu B_\mu$ by requiring that for $b \in B_\mu, b' \in B_{\mu'}$

$$b < b' \Leftrightarrow \mu \triangleright \mu'.$$

This defines a totally ordered basis of M and for $b \in B_\mu, b' \in B_{\mu'}$ we have (using $\Theta_0 = id$)

$$\Theta(b \otimes b') = f(\mu', \mu) \left(b' \otimes b + \sum_{\nu > 0} \Theta_\nu(b' \otimes b) \right) \in f(\mu', \mu) b' \otimes b + \sum_{\nu \triangleleft \mu'} M_\nu \otimes M$$

showing that the braiding is indeed left triangular. In the same one sees that the braiding is also right triangular.

We thank the referee for pointing out the following example.

Example 19 Assume that k is algebraically closed. Let G be an abelian group and $V \in {}^G\mathcal{YD}$ a Yetter-Drinfel'd module over G . Then the induced braiding

$$c : V \otimes V \rightarrow V \otimes V, \quad c(v \otimes w) = v_{(-1)} w \otimes v_{(0)}$$

is left triangular.

PROOF. For all $g \in G$ let $V_g := \{v \in V | \delta(v) = g \otimes v\}$. Then the V_g are G -submodules of V . As every simple submodule of a finite dimensional G module

is one dimensional we see that each V_g has a flag of invariant subspaces. So for all $g \in G$ we find a basis $v_1^g, \dots, v_{r_g}^g$ of V_g such that for all $h \in G$

$$h \cdot v_i^g \in kv_i^g \oplus \dots \oplus kv_{r_g}^g.$$

Now by concatenating these bases and ordering each according to the indices we obtain a totally ordered basis such that c is triangular. \square

In the previous example we used

Lemma 20 *Let G be an abelian group and V a finite dimensional simple representation of G . Then V is onedimensional.*

PROOF. Let V be a finite dimensional simple G module. By Schurs lemma (and because k is algebraically closed) there are scalars $\lambda_g \in k \setminus \{0\}$ such that for all $g \in G, v \in V$

$$gv = \lambda_g v.$$

So every $v \in V$ spans a onedimensional submodule. As V is simple we have that V is onedimensional. \square

Trivial but useful examples of left (and right) triangular endomorphisms are *diagonal braidings*. These are braidings d of $V \otimes V$ such that there is a basis $X \subset V$ and coefficients $\alpha_{x,y} \in k$ satisfying for all $x, y \in X$.

$$d(x \otimes y) = \alpha_{x,y} y \otimes x$$

In this case we have for arbitrary words $u, v \in \mathbb{X}$

$$d(u \otimes v) = \alpha_{u,v} v \otimes u,$$

where the coefficients $\alpha_{u,v}$ are defined inductively for all $x \in X$ by

$$\alpha_{1,1} = 1, \alpha_{x,1} = 1 = \alpha_{1,x}$$

and for all $u, u', v, v' \in \mathbb{X}$ by

$$\alpha_{uu',v} = \alpha_{u,v} \alpha_{u',v} \text{ resp. } \alpha_{u,vv'} = \alpha_{u,v} \alpha_{u,v'}.$$

Assume V is a vector space and r an endomorphism of $V \otimes V$ that is left triangular with respect to a basis $X \subset V$. Define the endomorphism $d : V \otimes V \rightarrow V \otimes V$ by

$$d(x \otimes y) = \gamma_{x,y} y \otimes x \text{ for all } x, y \in X,$$

where the coefficients $\gamma_{x,y}$ are those occuring in definition 15 for r . This endomorphism is a braiding and is called the *diagonal component* of r .

Remark 21 There are braidings that are triangular but not diagonal. For example the braiding on the simple twodimensional $U_q(\mathfrak{sl}_2)$ module (M, c) is left and right triangular, but not diagonal. Observe that if c was diagonal with respect to some basis A and diagonal coefficients $\alpha_{a,b}, a, b \in A$, then c would be diagonalizable as endomorphism of $M \otimes M$ with eigenvalues $\pm \sqrt{\alpha_{a,b}\alpha_{b,a}}$ for $b \neq a$ (eigenvectors $\sqrt{\alpha_{b,a}}a \otimes b \pm \sqrt{\alpha_{a,b}}b \otimes a$) resp. $\alpha_{a,a}$. But the eigenvalues of c in our case are -1 and q^{-2} . As we assumed q not to be a root of unity, the braiding can not be diagonal.

In [1] the case of diagonal braidings is studied. The central problem of this section is to generalize results of the diagonal case and to provide new tools necessary in the triangular case. The next lemma for example is trivial in the diagonal case.

Lemma 22 *Let V be a vector space and assume that c is a left triangular endomorphism with respect to the basis X . We have for words $u, v \in \mathbb{X}$:*

$$c(u \otimes v) \in d(u \otimes v) + k\mathbb{X}_{>v}^{l(v)} \otimes k\mathbb{X}^{l(u)},$$

where d is the diagonal component of c .

PROOF. We use double induction on $l(u)$ and $l(v)$. For $l(u) = 0$ and for $l(v) = 0$ the claim is trivial. So from now on assume $l(u), l(v) > 0$. If $l(u) = l(v) = 1$ the claim is exactly the condition from definition 15. Now let $l(u) = 1, l(v) > 1$ and write $v = xw$ with $x \in X, w \in \mathbb{X}$. Use the notation from definition 15. Then with $q := l(v)$ the induction hypothesis gives

$$\begin{aligned} c_{1,q}(u \otimes v) &= (\text{id}_V \otimes c_{1,q-1})(c_{1,1}(u \otimes x) \otimes w) \\ &= \gamma_{u,x}(\text{id} \otimes c_{1,q-1})((x \otimes u) \otimes w) \\ &\quad + \sum_{z > x} (\text{id} \otimes c_{1,q-1})((z \otimes v_{u,x,z}) \otimes w) \\ &\in \gamma_{u,x}\gamma_{u,w}x \otimes w \otimes u + \sum_{z > x} z \otimes k\mathbb{X}^{q-1} \otimes k\mathbb{X}^1 \\ &\subset \gamma_{u,xw}xw \otimes u + k\mathbb{X}_{>xw}^q \otimes k\mathbb{X}^1, \end{aligned}$$

where the last inclusion follows from the definition of the lexicographical order (note that in any case only words of the same length are compared). So now assume $q = l(v) \geq 1, p := l(u) > 1$ and write $u = wx$ for some $x \in X$. Then

$$\begin{aligned} c_{p,q}(u \otimes v) &= (c_{p-1,q} \otimes \text{id}_V)(w \otimes c_{1,q}(x \otimes v)) \\ &\in \gamma_{x,v}c_{p-1,q}(w \otimes v) \otimes x + c_{p-1,q}(w \otimes k\mathbb{X}_{>v}^q) \otimes k\mathbb{X}^1 \\ &\subset \gamma_{x,v}\gamma_{w,v}v \otimes wx + k\mathbb{X}_{>v}^q \otimes k\mathbb{X}^{p-1} \otimes x + k\mathbb{X}_{>v}^q \otimes k\mathbb{X}^p \end{aligned}$$

using the induction hypothesis for p twice. \square

Notation 23 Let (V, c) be a braided vector space that is left triangular with respect to a basis X . An endomorphism r of $V \otimes V$ will be called admissible if it satisfies the braid equation and is left triangular with respect to the basis X .

For example the braiding c itself, braidings which are diagonal with respect to the basis X and the zero morphism are admissible. The concept of commutators induced by admissible endomorphism allows us to formulate the process Kharchenko [21] refers to as monomial crystallization, namely the transfer from a basis of iterated commutators to a basis made up of the underlying words. The first part of the following lemma is a generalization of the second part of [1, Lemma 5] to our case of commutators coming from arbitrary admissible endomorphisms.

Lemma 24 Let (V, c) be a left triangular braided vector space with basis X and r an admissible endomorphism. Then for every word $u \in \mathbb{X}$ the polynomial $[u]_r$ is homogenous of degree $l(u)$ and the smallest monomial in this term is u with coefficient 1:

$$[u]_r \in u + k\mathbb{X}_{>u}^{l(u)}.$$

In particular if the diagonal component of the braiding c has the coefficients $\gamma_{x,y}$ and r is itself diagonal, we have

$$c([u]_r \otimes [v]_r) \in \gamma_{u,v}[v]_r \otimes [u]_r + k\mathbb{X}_{>v}^{l(v)} \otimes k\mathbb{X}^{l(u)}.$$

PROOF. Proceed by induction on $l(u)$. The cases $l(u) = 0, 1$ follow from the definition of $[-]_r$. In the case $l(u) > 1$ first assume u is a Lyndon word. Then we have a Shirshov decomposition $u = vw$ of u . With $p := l(v), q := l(w)$ (m is the multiplication map) we have

$$[u]_r = [v]_r[w]_r - mr_{p,q}([v]_r \otimes [w]_r)$$

and using the induction assumption we obtain

$$\begin{aligned} [u]_r &\in (v + k\mathbb{X}_{>v}^p)(w + k\mathbb{X}_{>w}^q) - mr_{p,q}(k\mathbb{X}^p \otimes k\mathbb{X}_{\geq w}^q) \\ &\subset vw + vk\mathbb{X}_{>w}^q + k\mathbb{X}_{>v}^p k\mathbb{X}_{\geq w}^q + k\mathbb{X}_{\geq w}^q k\mathbb{X}^p. \end{aligned}$$

Using the definition of the lexicographical order we see that the first and second subspace are contained $k\mathbb{X}_{>u}^{l(u)}$. For the third subspace take $a \in k\mathbb{X}_{\geq w}^q, b \in k\mathbb{X}^p$. Then (because u is Lyndon) $a \geq w > u$ and because a is shorter than u we obtain $ab > u$. Thus

$$[u]_r \in u + k\mathbb{X}_{>u}^{p+q}.$$

Now assume u is not Lyndon. Let $u = u_1 \dots u_t$ be the Lyndon decomposition and let $v := u_1, w := u_2 \dots u_t$ and $p := l(v), q := l(w)$. Then

$$\begin{aligned} [u]_r &= [v]_r [w]_r \in (v + k\mathbb{X}_{>v}^p)(w + k\mathbb{X}_{>w}^q) \\ &\subset vw + vk\mathbb{X}_{>w}^q + k\mathbb{X}_{>v}^p k\mathbb{X}^q \subset u + k\mathbb{X}_{>u}^{p+q}. \end{aligned}$$

For the second part observe that if r is diagonal then $[u]_r$ is just a linear combination of words u' that are obtained from the word u by permuting the letters of u . If also v' is obtained from v by permuting we have $\gamma_{u',v'} = \gamma_{u,v}$. Thus the diagonal part of c acts on every monomial in $[u]_r \otimes [v]_r$ by multiplication with $\gamma_{u,v}$. Together with the preceding lemma and the first part this completes the proof. \square

5 The comultiplication in the tensor algebra

Now in preparation of the final theorem we will prove some combinatorial properties of the comultiplication of the tensor algebra of a left triangular braided vector space. So for this section fix a finite dimensional braided vector space (V, c) , assume that it is left triangular with respect to the basis X and denote by d the diagonal component of c . Abbreviate $[-] := [-]_{d^{-1}}$ using the inverse of the diagonal component (As c is bijective it is easy to prove that the diagonal coefficients of c are not zero).

The technical lemmas in this section are motivated by similar calculations done in [1] in the case of diagonal braidings. A key idea is to use the iterated commutators induced by the inverse of the diagonal component of the braiding. Just using c or its inverse is not possible. The following lemma - a generalization of [1, lemma 8] - requires this. As Kharchenko works with diagonal braiding he can use the inverse of the braiding itself for the commutator. It is a central observation that it does not matter in fact which admissible endomorphism one uses for the commutator. If the final theorem is proved for some admissible endomorphism r it generalizes easily to any other admissible endomorphism (see remark 41).

Lemma 25 *Let $u \in \mathbb{X}$ be a Lyndon word and $n := l(u)$. Then*

$$\Delta([u]) \in [u] \underline{\otimes} 1 + 1 \underline{\otimes} [u] + \sum_{\substack{i+j=n \\ i,j \neq 0}} k\mathbb{X}_{>u}^i \underline{\otimes} k\mathbb{X}^j.$$

PROOF. Induction on $n = l(u)$. For $n = 1$ nothing has to be proved. Assume $n > 1$ and let $u = vw$ be the Shirshov decomposition of u . By induction we

have

$$\Delta([v]) \in [v] \underline{\otimes} 1 + 1 \underline{\otimes} [v] + \sum_{\substack{i+j=l(v) \\ i,j \neq 0}} k\mathbb{X}_{>v}^i \underline{\otimes} k\mathbb{X}^j \text{ and}$$

$$\Delta([w]) \in [w] \underline{\otimes} 1 + 1 \underline{\otimes} [w] + \sum_{\substack{l+m=l(w) \\ l,m \neq 0}} k\mathbb{X}_{>w}^l \underline{\otimes} k\mathbb{X}^m.$$

Now we obtain

$$\begin{aligned} \Delta([v])\Delta([w]) &\in \left([v] \underline{\otimes} 1 + 1 \underline{\otimes} [v] + \sum_{\substack{i+j=l(v) \\ i,j \neq 0}} k\mathbb{X}_{>v}^i \underline{\otimes} k\mathbb{X}^j \right) \cdot \\ &\quad \left([w] \underline{\otimes} 1 + 1 \underline{\otimes} [w] + \sum_{\substack{l+m=l(w) \\ l,m \neq 0}} k\mathbb{X}_{>w}^l \underline{\otimes} k\mathbb{X}^m \right) \\ &\subset [v][w] \underline{\otimes} 1 + [v] \underline{\otimes} [w] + 1 \underline{\otimes} [v][w] + \sum_{\substack{i+j=n \\ i,j \neq 0}} k\mathbb{X}_{>u}^i \underline{\otimes} k\mathbb{X}^j \end{aligned}$$

using the following facts:

$([v] \underline{\otimes} 1)(k\mathbb{X}_{>w}^i \underline{\otimes} k\mathbb{X}^j) \subset [v]k\mathbb{X}_{>w}^i \underline{\otimes} k\mathbb{X}^j \subset k\mathbb{X}_{>u}^{i+l(v)} \underline{\otimes} k\mathbb{X}^j$ by definition of the lexicographical order. As $w > u$ as u is Lyndon we have

$$(1 \underline{\otimes} [v])([w] \underline{\otimes} 1) = c([v] \underline{\otimes} [w]) \in k\mathbb{X}_{\geq w}^{l(w)} \underline{\otimes} k\mathbb{X}^{l(v)} \subset k\mathbb{X}_{>u}^{l(w)} \underline{\otimes} k\mathbb{X}^{l(v)}.$$

Furthermore $(1 \underline{\otimes} [v])(k\mathbb{X}_{>w}^l \underline{\otimes} k\mathbb{X}^m) \subset k\mathbb{X}_{>w}^l \underline{\otimes} k\mathbb{X}^{i+l(v)} \subset k\mathbb{X}_{>u}^l \underline{\otimes} k\mathbb{X}^{i+l(v)}$ using the same argument. Finally for all $i, j, l, m \in \mathbb{N}$ with $i < l(v)$ we have $(k\mathbb{X}_{>v}^i \underline{\otimes} k\mathbb{X}^j)(k\mathbb{X}_{>v}^l \underline{\otimes} k\mathbb{X}^m) \subset k\mathbb{X}_{>v}^i k\mathbb{X}_{>v}^l \underline{\otimes} k\mathbb{X}^{j+m} \subset k\mathbb{X}_{>u}^{i+l} \underline{\otimes} k\mathbb{X}^{j+m}$ because if $a \in \mathbb{X}$ is shorter than v and $a > v$ then for all $b \in \mathbb{X}$ also $ab > vb$.

On the other hand

$$\begin{aligned} \Delta([w])\Delta([v]) &\in \left([w] \underline{\otimes} 1 + 1 \underline{\otimes} [w] + \sum_{\substack{i+j=l(w) \\ i,j \neq 0}} k\mathbb{X}_{>w}^i \underline{\otimes} k\mathbb{X}^j \right) \cdot \\ &\quad \left([v] \underline{\otimes} 1 + 1 \underline{\otimes} [v] + \sum_{\substack{l+m=l(v) \\ l,m \neq 0}} k\mathbb{X}_{>v}^l \underline{\otimes} k\mathbb{X}^m \right) \\ &\subset [w][v] \underline{\otimes} 1 + d([w] \underline{\otimes} [v]) + 1 \underline{\otimes} [w][v] + \sum_{\substack{i+j=n \\ i,j \neq 0}} k\mathbb{X}_{>u}^i \underline{\otimes} k\mathbb{X}^j \end{aligned}$$

using $([w] \underline{\otimes} 1)(1 \underline{\otimes} [v]) = [w] \underline{\otimes} [v] \in k\mathbb{X}_{\geq w}^{l(w)} \underline{\otimes} k\mathbb{X}^{l(v)} \subset k\mathbb{X}_{>u}^{l(w)} \underline{\otimes} k\mathbb{X}^{l(v)}$ because again $w > u$ and $([w] \underline{\otimes} 1)(k\mathbb{X}_{>v}^i \underline{\otimes} k\mathbb{X}^j) \subset [w]k\mathbb{X}_{>v}^i \underline{\otimes} k\mathbb{X}^j \subset k\mathbb{X}_{>wv}^{l(w)+i} \underline{\otimes} k\mathbb{X}^j \subset k\mathbb{X}_{>u}^{i+l(w)} \underline{\otimes} k\mathbb{X}^j$ because u is Lyndon and thus $wv > vw = u$.

Next $(1 \otimes [w])([v] \otimes 1) = c([w] \otimes [v]) \in d([w] \otimes [v]) + k\mathbb{X}_{>w}^{l(w)} \otimes k\mathbb{X}^{l(v)} \subset d([w] \otimes [v]) + k\mathbb{X}_{>u}^{l(w)} \otimes k\mathbb{X}^{l(v)}$. Finally $k\mathbb{X}_{>w}, k\mathbb{X}_{>v}^i \subset k\mathbb{X}_{>u}$ if $i < l(v)$ and $k\mathbb{X}_{>u} \otimes k\mathbb{X}$ is a right ideal in $k\mathbb{X} \otimes k\mathbb{X}$. As $d([w] \otimes [v]) = \gamma_{w,v}[v] \otimes [w]$ we obtain

$$\begin{aligned} \Delta([u]) &= \Delta([v])\Delta([w]) - \gamma_{w,v}^{-1}\Delta([w])\Delta([v]) \\ &\in 1 \otimes [u] + [u] \otimes 1 + \sum_{\substack{i+j=n \\ i,j \neq 0}} k\mathbb{X}_{>u}^i \otimes k\mathbb{X}^j. \end{aligned}$$

□

To describe the comultiplication on arbitrary words we need an other subset of \mathbb{X} .

Definition 26 For $u, v \in \mathbb{X}$, u a Lyndon word we write $v \gg u$ if u is smaller than the first Lyndon letter of v . Furthermore $\mathbb{X}_{\gg u} := \{v \in \mathbb{X} | v \gg u\}$, $\mathbb{X}_{\gg u}^m := \mathbb{X}^m \cap \mathbb{X}_{\gg u}$.

Considering this subset is one of the key ideas in the step from the setting of diagonal braidings to that of triangular braidings. It can not be found in the work of Kharchenko. First we collect some auxiliary statements.

Remark 27 Let $u, v \in \mathbb{X}$, u a Lyndon word. Then:

- (1) $\mathbb{X}_{\gg u} = \{v \in \mathbb{X} | \text{ for all } i \in \mathbb{N} : v > u^i\}$.
- (2) If also v is Lyndon $v > u$ implies $v \gg u$.
- (3) If $v \gg u$, then $\mathbb{X}_{\geq v} \subset \mathbb{X}_{\gg u}$.
- (4) If v is Lyndon, $v > u$ then $\mathbb{X}_{\geq v}\mathbb{X} \subset \mathbb{X}_{\gg u}$.
- (5) If v is Lyndon, $v > u$ then $\mathbb{X}_{\gg v} \subset \mathbb{X}_{\gg u}$.
- (6) If $v > u$ and $l(v) \leq l(u)$ then $v \gg u$.
- (7) $\mathbb{X}_{\gg u}\mathbb{X} \subset \mathbb{X}_{\gg u}$.
- (8) If $i \in \mathbb{N}$ then $\mathbb{X}_{\geq u^i}^{il(u)} \mathbb{X}_{\gg u} \subset \mathbb{X}_{\gg u}$.

PROOF. For part 1 assume first that $v \gg u$ and let $v = v_1 \dots v_r$ be the Lyndon decomposition of v . This means that $v_1 > u$ by assumption and for all $i \in \mathbb{N}$ we obtain $v = v_1 \dots v_r > u^i$ by comparing the Lyndon letters lexicographically, keeping in mind that the Lyndon decomposition of u^i consist of i Lyndon letters u . On the other hand let $v \in \mathbb{X}$ with $v > u^i$ for all $i \in \mathbb{N}$. Again let $v = v_1 \dots v_r$ be the Lyndon decomposition. Because of $v > u$ we have $v_1 \geq u$. Assume $v_1 = u$. Then we find $i \in \mathbb{N}$ such that $v_1 = \dots = v_i = u$ and $v_{i+1}, \dots, v_r < u$. If $i = r$ we have $v = u^r < u^{r+1}$, a contradiction. If $i < r$ we have $v = u^i v_{i+1} \dots v_r < u^{i+1}$ by comparing the Lyndon letters - again a contradiction. Thus $v_1 > u$ and $v \gg u$. Part 2 follows from the definition. Part 3: Let $w \in \mathbb{X}, w \geq v$. Then $w \geq v > u^i$ for all $i \in \mathbb{N}$ and so $w \in \mathbb{X}_{\gg u}$. For part 4 consider $a, b \in \mathbb{X}$ with $a \geq v$. Then

$ab \geq a \geq v > u^i$ for all $i \in \mathbb{N}$. Part 5 is trivial.

Part 6: If v is Lyndon, this is part 2. Otherwise let $v = v_1 \dots v_r$ be the Lyndon decomposition of v . Then $v_1 \geq u$ and $l(v_1) < l(v) \leq l(u)$. So $v_1 > u$ and $v \gg u$.

For part 7 let $a \in \mathbb{X}_{\gg u}, b \in \mathbb{X}$. Let c be the first Lyndon letter of a . So we have $a \geq c > u$ and $ab \in \mathbb{X}_{\geq c} \mathbb{X} \subset \mathbb{X}_{\gg u}$ by part 4. Part 8: Assume $a \geq u^i, l(a) = il(u) = l(u^i), b \gg u$. First assume $j \geq i$. Then $ab \geq u^i b$ (because a and u^i have the same length) and $b > u^{j-i}$ and together $ab \geq u^i b > u^i u^{j-i} = u^j$. Now assume $j < i$. If u^j is the beginning of a , then also of ab and thus $ab > u^j$. If otherwise u^j is not the beginning of a , then $u^j < a$ (because $u^i \leq a$) implies $u^j < ab$. In any case $ab > u^j$ and thus $ab \gg u$. \square

Remark 28 Let $u \in \mathbb{X}$, u a Lyndon word and $p, q \in \mathbb{N}$. Then

$$c(k\mathbb{X}^p \underline{\otimes} k\mathbb{X}_{\gg u}^q) \subset k\mathbb{X}_{\gg u}^q \underline{\otimes} k\mathbb{X}^p.$$

PROOF. Let $v, w \in \mathbb{X}, v \gg u, l(v) = q, l(w) = p$. Then

$$c(w \underline{\otimes} v) \in k\mathbb{X}_{\geq v}^q \underline{\otimes} k\mathbb{X}^p \subset k\mathbb{X}_{\gg u}^q \underline{\otimes} k\mathbb{X}^p.$$

The last inclusion is by part 3 of the preceding remark. \square

Corollary 29 Let $u \in \mathbb{X}$ be a Lyndon word, $n = l(u)$. Then

$$\Delta([u]) \in [u] \underline{\otimes} 1 + 1 \underline{\otimes} [u] + \sum_{\substack{i+j=n \\ i,j \neq 0}} k\mathbb{X}_{\gg u}^i \underline{\otimes} k\mathbb{X}^j.$$

PROOF. By lemma 25 because Δ is graded we obtain

$$\Delta([u]) \in [u] \underline{\otimes} 1 + 1 \underline{\otimes} [u] + \sum_{\substack{i+j=n \\ i,j \neq 0}} k\mathbb{X}_{>u}^i \underline{\otimes} k\mathbb{X}^j,$$

but for $i < l(u) = n$ we have by part 6 of remark 27 $k\mathbb{X}_{>u}^i \subset k\mathbb{X}_{\gg u}^i$. \square

Thus up to terms of a special form (simple tensors whose left tensorand is made up of monomials having a first Lyndon letter bigger than u) the $[u]$ behave like primitive elements. The aim of this section is to extend this observation. In this spirit the next two lemmas are generalizations of calculations used in [1] to our situation. The more general context asks for a more careful formulation of statements and proofs.

Lemma 30 Let $v \in \mathbb{X}$ be a Lyndon word, $r \in \mathbb{N}$ and $n := l(v^r)$. Then

$$\Delta([v^r]) \in \sum_{i=0}^r \binom{r}{i}_{\gamma_{v,v}} [v]^i \underline{\otimes} [v]^{r-i} + \sum_{\substack{i+j=n \\ i,j \neq 0}} k\mathbb{X}_{\gg v}^i \underline{\otimes} k\mathbb{X}^j.$$

PROOF. We use induction on r . The case $r = 1$ is the preceding corollary. So assume $r > 1$. Then

$$\begin{aligned} \Delta([v^r]) &= \Delta([v]^{r-1})\Delta([v]) \\ &\in \left(\sum_{i=0}^{r-1} \binom{r-1}{i}_{\gamma_{v,v}} [v]^i \underline{\otimes} [v]^{r-1-i} + \sum_{\substack{i+j=n-l(v) \\ i,j \neq 0}} k\mathbb{X}_{\gg v}^i \underline{\otimes} k\mathbb{X}^j \right) \\ &\quad \left([v] \underline{\otimes} 1 + 1 \underline{\otimes} [v] + \sum_{\substack{l+m=l(v) \\ l,m \neq 0}} k\mathbb{X}_{\gg v}^l \underline{\otimes} k\mathbb{X}^m \right). \end{aligned}$$

Now note that $[v]^i k\mathbb{X}_{\gg v} \subset k\mathbb{X}_{\gg v}$ by part 8 of remark 27 and that thus $k\mathbb{X}_{\gg v} \underline{\otimes} k\mathbb{X}$ is stable under left multiplication with elements from $[v]^i \underline{\otimes} k\mathbb{X}$. Furthermore $k\mathbb{X}_{\gg v} \underline{\otimes} k\mathbb{X}$ is a right ideal in $k\mathbb{X} \underline{\otimes} k\mathbb{X}$. As (again by part 8 of remark 27)

$$\begin{aligned} ([v]^i \underline{\otimes} [v]^j)([v] \underline{\otimes} 1) &= \gamma_{v,v}^j [v]^{i+1} \underline{\otimes} [v]^j + k\mathbb{X}_{>v^{i+1}}^{l(v^{i+1})} \underline{\otimes} k\mathbb{X}^{l(v^k)} \\ &\subset \gamma_{v,v}^j [v]^{i+1} \underline{\otimes} [v]^j + k\mathbb{X}_{\gg v}^{l(v^{i+1})} \underline{\otimes} k\mathbb{X}^{l(v^k)} \end{aligned}$$

this implies

$$\Delta([v^r]) \in \sum_{i=0}^{r-1} \binom{r-1}{i}_{\gamma_{v,v}} \left(\gamma_{v,v}^i [v]^{i+1} \underline{\otimes} [v]^{r-1-i} + [v]^i \underline{\otimes} [v]^{r-i} \right) + \sum_{\substack{i+j=n \\ i,j \neq 0}} k\mathbb{X}_{\gg v}^i \underline{\otimes} k\mathbb{X}^j$$

and using the recursion formula for the q -binomial coefficients we obtain the claim. \square

Lemma 31 *Let $u \in \mathbb{X}$ and $u = u_1 \dots u_t v^r$, $u_1 \geq \dots \geq u_t > v$ be the Lyndon decomposition with $r, t \geq 1$. Define $z := u_1 \dots u_t$, $n := l(u)$. Then*

$$\Delta([u]) \in [u] \underline{\otimes} 1 + \sum_{i=0}^r \binom{r}{i}_{\gamma_{v,v}} \gamma_{z,v}^i [v]^i \underline{\otimes} [z][v]^{r-i} + \sum_{\substack{i+j=n \\ i,j \neq 0}} k\mathbb{X}_{\gg v}^i \underline{\otimes} k\mathbb{X}^j.$$

PROOF. We use induction on t . First assume $t = 1$. Then z is Lyndon and $z > v$. By part 5 of remark 27 we have $k\mathbb{X}_{\gg z} \subset k\mathbb{X}_{\gg v}$. So we obtain using the preceding lemma

$$\begin{aligned}
\Delta([zv^r]) &= \Delta([z])\Delta([v]^r) \\
&\in \left([z]\underline{\otimes}1 + 1\underline{\otimes}[z] + \sum_{\substack{i+j=l(z) \\ i,j \neq 0}} k\mathbb{X}_{\gg v}^i \underline{\otimes} k\mathbb{X}^j \right) \\
&\quad \left(\sum_{i=0}^r \binom{r}{i} \gamma_{v,v} [v]^i \underline{\otimes} [v]^{r-i} + \sum_{\substack{l+m=l(v^r) \\ l,m \neq 0}} k\mathbb{X}_{\gg v}^l \underline{\otimes} k\mathbb{X}^m \right).
\end{aligned}$$

Again $k\mathbb{X}_{\gg v} \underline{\otimes} k\mathbb{X}$ is a right ideal and stable under left multiplication with $1\underline{\otimes}[z]$.

Moreover by part 8 of remark 27 $(1\underline{\otimes}[z])([v]^i \underline{\otimes} [v]^{r-i}) \in \gamma_{z,v}^i [v]^i \underline{\otimes} [z][v]^{r-i} + k\mathbb{X}_{>v^i}^{l(v^i)} \underline{\otimes} k\mathbb{X}^{n-l(v^i)} \subset \gamma_{z,v}^i [v]^i \underline{\otimes} [z][v]^{r-i} + k\mathbb{X}_{\gg v}^{l(v^i)} \underline{\otimes} k\mathbb{X}^{n-l(v^i)}$. As furthermore $[z] \in k\mathbb{X}_{\geq z} \subset k\mathbb{X}_{\gg v}$ (part 3 of remark 27) we obtain

$$\Delta([u][v^r]) \in [u][v]^r \underline{\otimes} 1 + \sum_{i=0}^r \binom{r}{i} \gamma_{v,v}^i [v]^i \underline{\otimes} [z][v]^{r-i} + \sum_{\substack{i+j=n \\ i,j \neq 0}} k\mathbb{X}_{\gg v}^i \underline{\otimes} k\mathbb{X}^j.$$

So assume now $t > 1$ and let $w := u_2 \dots u_t$. The induction hypothesis and the preceding lemma give

$$\begin{aligned}
\Delta([u_1]) &\in [u_1]\underline{\otimes}1 + 1\underline{\otimes}[u_1] + \sum_{\substack{i+j=l(u) \\ i,j \neq 0}} k\mathbb{X}_{\gg v}^i \underline{\otimes} k\mathbb{X}^j \\
\Delta([z][v]^r) &\in [z][v]^r \underline{\otimes} 1 + \sum_{i=0}^r \binom{r}{i} \gamma_{w,v}^i [v]^i \underline{\otimes} [w][v]^{r-i} \\
&\quad + \sum_{\substack{l+m=l(v^r) \\ l,m \neq 0}} k\mathbb{X}_{\gg v}^l \underline{\otimes} k\mathbb{X}^m.
\end{aligned}$$

Multiplying these we use that $k\mathbb{X}_{\gg v} \underline{\otimes} k\mathbb{X}$ is a right ideal and stable under left multiplication with elements from $k\mathbb{X}_{>v} \underline{\otimes} k\mathbb{X}$ and $1\underline{\otimes} k\mathbb{X}$. Note $[u_1] \in k\mathbb{X}_{\gg v}$, $[z][v]^r \in k\mathbb{X}_{\gg v}$. Together with

$$(1\underline{\otimes}[u_1])([v]^i \underline{\otimes} [z][v]^{r-i}) \in \gamma_{u_1,v}^i [v]^i \underline{\otimes} [u_1][z][v]^{r-i} + k\mathbb{X}_{\gg v}^{l(v^i)} \underline{\otimes} k\mathbb{X}^{n-l(v^i)}$$

we have

$$\begin{aligned}
\Delta([u_1][w][v]^r) &\in [u_1][w][v]^r \underline{\otimes} 1 + \sum_{i=0}^r \binom{r}{i} \gamma_{w,v}^i \gamma_{u_1,v}^i [v]^i \underline{\otimes} [u_1][w][v]^{r-i} \\
&\quad + \sum_{\substack{i+j=n \\ i,j \neq 0}} k\mathbb{X}_{\gg v}^i \underline{\otimes} k\mathbb{X}^j
\end{aligned}$$

establishing the claim. \square

6 A PBW basis for braided Hopf algebras with left triangular braiding

We will use the results of the preceding section to prove the existence of a PBW type basis made up of iterated skew commutators for a class of braided Hopf algebras. We start with a general definition of the term PBW basis.

Definition 32 *Let A be an algebra, $P, S \subset A$ subsets and $h : S \rightarrow \mathbb{N} \cup \{\infty\}$. Let $(S, <)$ be a totally ordered set. Let $B(P, S, <, h)$ be the set of all products*

$$s_1^{e_1} \dots s_t^{e_t} p$$

with $t \in \mathbb{N}_0, s_1 > \dots > s_t, s_i \in S, 0 < e_i < h(s_i)$ and $p \in P$. This set is called the PBW set generated by $P, (S, <)$ and h . h is called the height function of the PBW set.

We say $(P, S, <, h)$ is PBW basis of A if $B(P, S, <, h)$ is a basis of A .

Of course every algebra A has the trivial PBW basis with $S = \emptyset$ and P a basis of A . In the (braided) bialgebra case we are interested in the case that P is a basis of the coradical. Thus in this section we are interested in the case where $P = \{1\}$. We will say that $B(S, <, h) := B(\{1\}, S, <, h)$ is the PBW set (resp. PBW basis) generated by $(S, <)$ and h .

As in the preceding section fix a finite dimensional braided vector space (V, c) that is left triangular with respect to a basis X of V . Let d be the diagonal component of c and abbreviate $[-] := [-]_{d^{-1}}$. Identify $T(V)$ with $k\mathbb{X}$.

Definition 33 *Define the standard order in the following way. For two elements $u, v \in \mathbb{X}$ write $u \succeq v$ if and only if u is shorter than v or if $u \geq v$ lexicographically and $l(u) = l(v)$.*

In this order the empty word 1 is the maximal element. As X is assumed to be finite, this order fulfils the ascending chain condition, making way for inductive proofs. Define $\mathbb{X}_{>u}, \mathbb{X}_{\geq u}$ etc. in the obvious way.

Now we will define the PBW set that will lead to the PBW basis of our braided Hopf algebra. The sets S_I resp. B_I are analogues of the sets of “hard superletters” resp. of “monotonous words in hard superletters” found in [1].

Definition 34 *Let $I \subsetneq k\mathbb{X}$ be a biideal. Let S_I be the set of Lyndon words from \mathbb{X} that do not appear as (standard-) smallest monomial in elements of I :*

$$S_I := \{u \in \mathbb{X} \mid u \text{ is a Lyndon word and } u \notin k\mathbb{X}_{>u} + I\}.$$

For $u \in S_I$ define the height of $h_I(u) \in \{2, 3, \dots, \infty\}$ by

$$h_I(u) := \min\{t \in \mathbb{N} \mid u^t \in k\mathbb{X}_{>u^t} + I\}$$

and let $B_I := B(S_I, <, h_I)$ be the PBW set generated by $(S_I, <)$ and (h_I) , where $<$ denotes the lexicographical order.

If r is an admissible endomorphism of $V \otimes V$ and $U \subset \mathbb{X}$ is any subset define $[U]_r := \{[u]_r | u \in U\}$. Denote by $k[U]_r$ the k -linear subspace of $k\mathbb{X}$ spanned by $[U]_r$ (To avoid confusion with the notation for polynomial rings let me note that no polynomial rings will be considered during this section).

This section will mainly be devoted to the proof of the following central theorem. Note that in the special case of diagonal braidings this theorem together with lemma 42 is a braided analogue of [1, theorem 2].

Theorem 35 *Let (V, c) be a finite dimensional braided vector space that is left triangular with respect to some basis X . Identify $T(V)$ with $k\mathbb{X}$ and let $I \subsetneq k\mathbb{X}$ be a braided biideal, $\pi : k\mathbb{X} \rightarrow (k\mathbb{X})/I$ the quotient map. Then $\pi(B_I)$ and $\pi([B_I]_c)$ are bases of $(k\mathbb{X})/I$.*

These are the truncated PBW bases generated by $\pi(S_I)$ resp. $\pi([S_I]_c)$ with heights $h_I(u)$ for $u \in S_I$.

Remark 36 The reader should observe that in changing from diagonal to triangular braidings we lost some information on the basis. Kharchenko shows that in the diagonal case every reducible Lyndon word u is (modulo I) a linear combination of

- words of the same degree as u that are nonascending products in PBW generators lexicographically smaller than u and
- words of degree smaller than that of u that are nonascending products in arbitrary PBW generators.

It is an open question whether this (or something similar) can be done for triangular braidings.

6.1 Proof of theorem 35

We will omit the index corresponding to the subspace I during the technical parts of this section. So we can introduce some new notation: for $n \in \mathbb{N}$ and a Lyndon word $v \in \mathbb{X}$ define $B^n := B \cap \mathbb{X}^n$, $B_{\gg v} := B \cap \mathbb{X}_{\gg v}$ and $B_{\gg v}^n := B^n \cap B_{\gg v}$.

The next proposition collects some statements which will be useful in the sequel. Analogues of Parts 1,3 and 4 are also used in [1].

Proposition 37 *Let r be an admissible endomorphism of $V \otimes V$. For every $m \in \mathbb{N}_0$, $u, v \in \mathbb{X}$, v a Lyndon word we have the following inclusions*

- (1) $k\mathbb{X}_{\succeq u} \subset k[B_{\succeq u}]_r + I$,
- (2) $k\mathbb{X}_{\succcurlyeq v}^m \subset k[B_{\succcurlyeq v}^m]_r + \sum_{0 \leq i < m} k[B^i]_r + I$,
- (3) $k\mathbb{X}^m \subset \sum_{0 \leq i \leq m} k[B^i]_r + I$,
- (4) $k\mathbb{X} = k[\bar{B}]_r + I$.

PROOF. First note that for $x, y, a, b \in \mathbb{X}$ $a \succ b$ implies $xay \succ xby$. For part 1 we proceed by downward induction along the standard order (this works because the standard order satisfies the ascending chain condition). For $u = 1$ the inclusion is valid. Now assume $u \prec 1$ and that for all words $\succ u$ the inclusion is valid. Let $w \succeq u$, $m := l(w)$. If $w \in B$ we have $w \in [w]_r + k\mathbb{X}_{\succ w} \subset k[B_{\succeq w}]_r + I$ by induction. Assume $w \notin B$ and let $w = w_1^{e_1} \dots w_t^{e_t}$ be the Lyndon decomposition of w . As $w \notin B$ we find an $0 \leq i \leq t$ such that either $w_i \notin S$ or $e_i \geq h(w_i)$. In the first case we have $w_i \in k\mathbb{X}_{\succ w_i} + I$, in the second case $w_i^{e_i} \in k\mathbb{X}_{\succ w_i^{e_i}} + I$. Anyway this implies $w \in k\mathbb{X}_{\succ w} + I$, but thus $[w]_r \in k\mathbb{X}_{\succ w} + I \subset k[B_{\succ w}]_r + I \subset k[B_{\succ u}]_r + I$ by induction. Now for part 2 assume $w \in k\mathbb{X}_{\succcurlyeq v}^m$. Then by part 1 $w \in k\mathbb{X}_{\succeq w} \subset k[B_{\succeq w}]_r + I \subset k[B_{\succeq w}^m]_r + \sum_{0 \leq i < m} k[B^i]_r + I$. In view of 27 we have $k\mathbb{X}_{\succeq w}^m \subset k\mathbb{X}_{\succcurlyeq v}^m$, finishing the proof. For part 3 let u_0 be the smallest word of degree m . For $u \in \mathbb{X}^m$ we have $u \succeq u_0$ and thus by part 1 $u \in k[B_{\succeq u_0}]_r + I$ and this is a subset of $\sum_{0 \leq i \leq m} k[B^i]_r$. Finally Part 4 follows from Part 3. \square

For the rest of the proof we use the main ideas of [1], but in a different and more general setting. As the triangular braiding requires a more careful analysis we work in the tensor algebra rather than in the quotient of the tensor algebra by the ideal I (as Kharchenko does, not regarding the biproduct with the group algebra). This enables us to use linear maps as tools where Kharchenko argues by inspection of the occuring terms, a method for which our situation seems to be too complicated.

Lemma 38 *Let r be an admissible endomorphism of $V \otimes V$. Then the set $[B_I]_r$ is linearly independent.*

PROOF. The map $[-]_r : k\mathbb{X} \rightarrow k\mathbb{X}$ is homogenous. Furthermore it is surjective (use part 4 of the proposition above for the subspace (0) to see that $k\mathbb{X} = k[\mathbb{X}]_r$). As the homogenous components are finite dimensional, $[-]_r$ is bijective and maps the linearly independent set B_I onto $[B_I]_r$. So $[B_I]_r$ is linearly independent. \square

The next theorem is the key step to the final theorem combining the results of the preceeding section on the comultiplication with the results of this section.

Theorem 39 *Let $I \subsetneq k\mathbb{X}$ be a braided biideal in $k\mathbb{X}$. Then $[B_I]$ spans a k -linear complement of I .*

PROOF. By the proposition above all we need to show is that $k[B_I]$ and I have trivial intersection. For $n \geq 0$ let $U_n := \text{k-span}\{[u] | u \in B_I, l(u) \leq n\}$. We show by induction on n that for all $n \in \mathbb{N}$ we have $U_n \cap I = (0)$. First let $n = 0$. Then $U_0 = k1$ and I is proper ideal, so $U_0 \cap I = (0)$. Now assume $n > 0$. Assume $0 \neq T \in U_n \cap I$. So we can write T as a (finite) sum

$$T = \sum_{\substack{u \in B_I \\ l(u) \leq n}} \alpha_u [u].$$

We may assume that there is a $u \in B^n$ such that $\alpha_u \neq 0$. Now choose v as the (lexicographically) smallest Lyndon letter occuring in the Lyndon decomposition of words $u \in B_I^n$ with $\alpha_u \neq 0$. Because of the minimality of v , it occurs in Lyndon decompositions of words $u \in B_I^n$ with $\alpha_u \neq 0$ only at the end. Let t be the maximal number of occurrences of v in a Lyndon decomposition of word $u \in B_I^n$ with $\alpha_u \neq 0$. Thus we can decompose the sum for T in the following way

$$T = \sum_{u \in O} \alpha_u [a_u][v]^t + \sum_{u \in P} \alpha_u [a_u][v]^{t_u} + \sum_{u \in Q} \alpha_u [u] + \sum_{u \in R} \alpha_u [u],$$

where $O, P, Q, R \subset B_I$ and the words a_u for $u \in O \cup P$ are chosen such that

- O contains all words $u \in B_I^n$ of length n with $\alpha_u \neq 0$ such that the Lyndon decomposition of u ends with v^t . Furthermore $u = a_u v^t$.
- P contains all words $u \in B_I^n$ of length n with $\alpha_u \neq 0$ such that the Lyndon decomposition of u ends with v^{t_u} for some $0 \neq t_u < t$. Furthermore $u = a_u v^{t_u}$.
- Q contains all words $u \in B_I^n$ of length n with $\alpha_u \neq 0$ that do not have the Lyndon letter v in their Lyndon decomposition.
- R contains all words $u \in B_I^n$ of length less than n with $\alpha_u \neq 0$.

Note that for all $u \in O$ we have $a_u \neq 1$ as $u \in B$. By analyzing the four terms we will show

$$\begin{aligned} \Delta(T) \in T \underline{\otimes} 1 + [v]^t \underline{\otimes} \sum_{u \in O} \alpha_u \gamma_{a_u, v}^t [a_u] + \sum_{i=0}^{t-1} [v]^i \underline{\otimes} k\mathbb{X}^{n-l(v^i)} + \\ \sum_{\substack{i+j=n \\ i, j \neq n}} k[B_{\gg v}^i] \underline{\otimes} k\mathbb{X}^j + \sum_{i+j < n} k[B^i] \underline{\otimes} k\mathbb{X}^j + I \underline{\otimes} k\mathbb{X}. \end{aligned}$$

At first consider $u \in O, l := t$ or $u \in P, l := t_u < t$. Note that then $a_u \neq 1$: $a_u = 1$ would imply that $u = v^l \in k\mathbb{X}_{>v^l}$, but as well $l < h_I(v)$ because $u \in B$ which is a contradiction to the definition of $h_I(v)$. So we obtain

$$\begin{aligned}
\Delta([a_u][v]^l) &\in [a_u][v]^l \underline{\otimes} 1 + \sum_{i=0}^l \binom{l}{i} \gamma_{a_u, v}^i [v]^i \underline{\otimes} [a_u][v]^{l-i} + \sum_{\substack{i+j=n \\ i, j \neq 0}} k\mathbb{X}_{\gg v}^i \underline{\otimes} k\mathbb{X}^j \\
&\subset [a_u][v]^l \underline{\otimes} 1 + [v]^l \underline{\otimes} \gamma_{a_u, v}^l [a_u] + \sum_{i=0}^{l-1} [v]^i \underline{\otimes} k\mathbb{X}^{n-l(v^i)} + \\
&\quad \sum_{\substack{i+j=n \\ i, j \neq 0}} k[B_{\gg v}^i] \underline{\otimes} k\mathbb{X}^j + \sum_{i+j < n} k[B^i] \underline{\otimes} k\mathbb{X}^j + I \underline{\otimes} k\mathbb{X}.
\end{aligned}$$

In both cases ($u \in O$ or $u \in P$) this delivers the right terms in the sum for the word u . Now consider $u \in Q$ and let w be the largest Lyndon letter occuring in the Lyndon decomposition of u . Then $u = aw^l$ for some $l \in \mathbb{N}, a \in \mathbb{X}$ and $w > v$ by construction of v . This leads to

$$\begin{aligned}
\Delta([u]) &\in [u] \underline{\otimes} 1 + \sum_{i=0}^l \binom{l}{i} \gamma_{a, w}^i [w]^i \underline{\otimes} [a][w]^{l-i} + \sum_{\substack{i+j=n \\ i, j \neq 0}} k\mathbb{X}_{\gg w}^i \underline{\otimes} k\mathbb{X}^j \\
&\subset [u] \underline{\otimes} 1 + \sum_{\substack{i+j=n \\ i, j \neq 0}} k\mathbb{X}_{\gg v}^i \underline{\otimes} k\mathbb{X}^j \\
&\subset [u] \underline{\otimes} 1 + \sum_{\substack{i+j=n \\ i, j \neq 0}} k[B_{\gg v}^i] \underline{\otimes} k\mathbb{X}^j + \sum_{i+j < n} k[B^i] \underline{\otimes} k\mathbb{X}^j + I \underline{\otimes} k\mathbb{X}.
\end{aligned}$$

Finally consider $u \in R$. Then $l(u) < n$ and we obtain

$$\begin{aligned}
\Delta([u]) &\in [u] \underline{\otimes} 1 + \sum_{i+j < n} k\mathbb{X}^i \underline{\otimes} k\mathbb{X}^j \\
&\subset [u] \underline{\otimes} 1 + \sum_{i+j < n} k[B^i] \underline{\otimes} k\mathbb{X}^j + I \underline{\otimes} k\mathbb{X}.
\end{aligned}$$

Now by induction assumption we find a $\phi \in (k\mathbb{X})^*$ such that

$$\phi(I) = 0, \phi([v]^t) = 1 \text{ and } \forall u \in B \setminus \{v^t\} \text{ with } l(u) < n : \phi([u]) = 0.$$

With the inclusion showed above we get

$$\begin{aligned}
(\phi \underline{\otimes} \text{id})\Delta(T) &\in \sum_{u \in O} \alpha_u \gamma_{a_u, v}^t [a_u] + \sum_{\substack{i+j=n \\ i, j \neq 0}} \phi(k[B_{\gg v}^i]) k\mathbb{X}^j + \\
&\quad \sum_{i+j < n} \phi(k[B^i]) k\mathbb{X}^j + \phi(I) k\mathbb{X} \\
&\subset \sum_{u \in O} \alpha_u \gamma_{a_u, v}^t [a_u] + 0 + \sum_{j < n - tl(v)} k\mathbb{X}^j + 0 \\
&\subset \{k[B^{n-tl(v)}] \oplus U_{n-tl(v)-1}\} \setminus \{0\} \subset U_{n-1} \setminus \{0\}.
\end{aligned}$$

Note that we can not obtain 0, because we have a non-zero component in degree $n - tl(v)$. On the other hand, as I is a biideal, we have

$$(\phi \otimes \text{id})\Delta(T) \in \phi(I)k\mathbb{X} + \phi(k\mathbb{X})I \subset I.$$

Thus $(\phi \otimes \text{id})\Delta(T) \in I \cap (U_{n-1} \setminus \{0\})$, but by induction assumption this is the empty set, a contradiction. \square

Corollary 40 *Let $I \subsetneq k\mathbb{X}$ be a braided biideal and r an admissible endomorphism of $V \otimes V$. Then $[B_I]_r$ spans a k -linear complement of I .*

PROOF. Again all we have to show is that $k[B]_r \cap I = \{0\}$. Assume $0 \neq T \in k[B]_r \cap I$. We can write T as

$$T = \alpha[u]_r + \sum_{w \succ u} \beta_w[w]_r$$

with $\alpha \neq 0$. Then by the proposition 37 and lemma 24 we obtain first

$$T \in \alpha u + k\mathbb{X}_{\succ u}$$

and from this

$$T \in \alpha[u] + k\mathbb{X}_{\succ u} \subset \alpha[u] + k[B_{\succ u}] + I.$$

So now write $T = \alpha[u] + x + i$ with $x \in k[B_{\succ u}]$, $i \in I$. Now by the theorem above we obtain $\alpha[u] + x \in I \cap k[B] = \{0\}$. Thus $\alpha = 0$ because $[B]_r$ is linearly independent, a contradiction. \square

Now theorem 35 follows as a special case of the following remark.

Remark 41 *Let $I \subsetneq k\mathbb{X}$ be a braided biideal and r an admissible endomorphism of $V \otimes V$. Then $\pi([B_I]_r)$ is a basis of $(k\mathbb{X})/I$.*

PROOF. By corollary 40 $[B_I]_r$ is a basis for a complement of I . As $I = \ker \pi$, π induces a k -linear isomorphism $k[B_I]_r \rightarrow k\mathbb{X}/I$, mapping the basis $[B_I]_r$ into $\pi([B_I]_r)$. This proves the remark. The theorem follows by using $r = 0$ and $r = c$. \square

6.2 A result on the height function

The next lemma is useful to ensure that all elements of S_I have infinite height if $\text{char}(k) = 0$ and the diagonal coefficients of the braiding are powers of one element that is not a root of unity. Its analogue in the case of diagonal braidings is already contained in the definition of the height function in [1].

Lemma 42 *Let (V, c) be a finite dimensional braided vector space that is left triangular with respect to some basis X . Identify $T(V)$ with $k\mathbb{X}$ and let $I \subsetneq k\mathbb{X}$ be a braided biideal and $v \in S_I$. Define the scalar $\gamma_{v,v} \in k$ by*

$$d(v \otimes v) = \gamma_{v,v} v \otimes v$$

where d is the diagonal component of c .

If $h := h_I(v) < \infty$, then $\gamma_{v,v}$ is a root of unity. In this case let t be the order of $\gamma_{v,v}$. If $\text{char } k = 0$ then $\gamma_{v,v} \neq 1$ and $h = t$. If $\text{char } k = p > 0$ then $h = tp^l$ for some $l \in \mathbb{N}$.

PROOF. Let $n := l(v^h)$. We have an element of I of the form

$$T := [v]^h + \sum_{\substack{u > v^h \\ l(u)=n}} \alpha_u [u] + \sum_{l(w) < n} \alpha_w [w] \in I.$$

For every $u \in \mathbb{X}^n$ with $u > v^h$ we have $u \gg v$ and thus we obtain for the coproduct using lemmas 30 and 31

$$\begin{aligned} \Delta(T) &\in T \underline{\otimes} 1 + \sum_{i=0}^{h-1} \binom{h}{i}_{\gamma_{v,v}} [v]^i \underline{\otimes} [v]^{h-i} + \sum_{\substack{i+j=n \\ j \neq 0}} k\mathbb{X}_{\gg v}^i \underline{\otimes} k\mathbb{X}^j + \sum_{\substack{i+j < n \\ j \neq 0}} k\mathbb{X}^i \underline{\otimes} k\mathbb{X}^j \\ &\subset T \underline{\otimes} 1 + \sum_{i=0}^{h-1} \binom{h}{i}_{\gamma_{v,v}} [v]^i \underline{\otimes} [v]^{h-i} + \sum_{i+j=n} k[B_{\gg v}^i] \underline{\otimes} k[B^j] + \\ &\quad \sum_{i+j < n} k[B^i] \underline{\otimes} k[B^j] + I \underline{\otimes} k\mathbb{X} + k\mathbb{X} \underline{\otimes} I. \end{aligned}$$

Now because of $k\mathbb{X} \underline{\otimes} k\mathbb{X} = (I \underline{\otimes} k\mathbb{X} + k\mathbb{X} \underline{\otimes} I) \oplus (k[B] \underline{\otimes} k[B])$ we can construct a k -linear map $\phi_1 : k\mathbb{X} \otimes k\mathbb{X} \rightarrow k$ such that

$$\begin{aligned} \forall (b, b') \in (B \times B) \setminus \{(v, v^{h-1})\} : \phi_1([b] \underline{\otimes} [b']) &= 0, \\ \phi_1([v] \underline{\otimes} [v]^{h-1}) &= 1, \\ \phi_1(I \underline{\otimes} k\mathbb{X} + k\mathbb{X} \underline{\otimes} I) &= 0. \end{aligned}$$

As $T \in I$ we have $\phi_1 \Delta(T) = 0$ and on the other hand using what we proved above

$$0 = \phi_1 \Delta(T) = \binom{h}{h-1}_{\gamma_{v,v}} = 1 + \gamma_{v,v} + \dots + \gamma_{v,v}^{h-1}.$$

This shows that $\gamma_{v,v}$ is a root of unity, say of order t (set $t = 1$ if $\gamma_{v,v} = 1$). Let $p := \text{char } k$ and define q by

$$q := \begin{cases} p & \text{if } p > 0 \\ 1 & \text{if } p = 0. \end{cases}$$

Now we can write $h = tq^l a$ with $a, l \in \mathbb{N}$. If $q \neq 1$ we may assume that q does not divide a . We want to show that $a = 1$. So assume $a > 1$. In this case we can construct a k -linear map $\phi_2 : k\mathbb{X} \otimes k\mathbb{X} \rightarrow k$ with

$$\begin{aligned} \forall (b, b') \in (B \times B) \setminus \{(v^{tq^l}, v^{tq^l(a-1)})\} : \phi_2([b] \underline{\otimes} [b']) &= 0, \\ \phi_2([v]^{tq^l} \underline{\otimes} [v]^{tq^l(a-1)}) &= 1, \\ \phi_2(I \underline{\otimes} k\mathbb{X} + k\mathbb{X} \underline{\otimes} I) &= 0. \end{aligned}$$

Using that $\gamma_{v,v}$ is a primitive t -th root of unity (resp. $\gamma_{v,v} = 1$ and $t = 1$) we obtain that in k

$$0 = \phi_2 \Delta(T) = \begin{pmatrix} tq^l a \\ tq^l \end{pmatrix}_{\gamma_{v,v}} = \begin{pmatrix} q^l a \\ q^l \end{pmatrix} = \begin{pmatrix} a \\ 1 \end{pmatrix} = a.$$

This is a contradiction to the assumptions we made on a . Thus $h = tq^l$. In particular if $\text{char } k = 0$, then $q = 1$ and because $t = h > 1$ we obtain $\gamma_{v,v} \neq 1$. \square

7 Right triangular braidings

In principle one could do a similar proof as above for right triangular braidings, but an easy argument shows that the right triangular case follows from the left triangular case. Obviously c is a right triangular braiding if and only if $\tau c \tau$ is a left triangular braiding, where τ denotes the usual flip map. The key observation is

Proposition 43 *Let $(R, \mu, \eta, \Delta, \varepsilon, c)$ be a braided bialgebra. Then also $R^{op, cop} := (R, \mu\tau, \eta, \tau\Delta, \varepsilon, \tau c \tau)$ is a braided bialgebra.*

PROOF. Of course (R, μ^{op}, η) is an algebra, $(R, \Delta^{cop}, \varepsilon)$ is a coalgebra and $(R, \tau c \tau)$ is a braided vector space. Checking the compatibility of $\mu^{op}, \eta, \Delta^{cop}, \varepsilon$ with $\tau c \tau$ is tedious. We will do one example, namely the calculation that $\tau c \tau \circ (\mu^{op} \otimes R) = (R \otimes \mu^{op})(\tau c \tau \otimes R)(R \otimes \tau c \tau)$. We calculate

$$\begin{aligned}
& (R \otimes \mu^{op})(\tau c \tau \otimes R)(R \otimes \tau c \tau) = \\
& (R \otimes \mu) \underline{(R \otimes \tau)(\tau \otimes R)(R \otimes \tau)(R \otimes \tau)(c \tau \otimes R)(R \otimes \tau c \tau)} = \\
& \underline{(R \otimes \mu)(\tau \otimes R)(R \otimes \tau)} \circ \underline{(\tau \otimes R)(R \otimes \tau)(c \otimes R)(\tau \otimes R)(R \otimes \tau c \tau)} = \\
& \tau(\mu \otimes R) \circ (R \otimes c) \underline{(\tau \otimes R)(R \otimes \tau)(\tau \otimes R)(R \otimes \tau c \tau)} = \\
& \tau(\mu \otimes R)(R \otimes c) \underline{(R \otimes \tau)(\tau \otimes R)(R \otimes c)(R \otimes \tau)} = \\
& \underline{\tau(\mu \otimes R)(R \otimes c)(c \otimes R)} \circ \underline{(R \otimes \tau)(\tau \otimes R)(R \otimes \tau)} = \\
& \tau c \underline{(R \otimes \mu) \circ (\tau \otimes R)(R \otimes \tau)(\tau \otimes R)} = \\
& \tau c \tau (\mu \otimes R)(\tau \otimes R) = \\
& \tau c \tau (\mu^{op} \otimes R),
\end{aligned}$$

where we use (in this order): $\tau^2 = \text{id}_{V \otimes V}$, the braid equation for τ, μ, c commute with τ , again the braid equation for τ and $\tau^2 = \text{id}_{V \otimes V}$, c commutes with τ , μ commutes with c and the braid equation for τ and finally again that μ commutes with τ . The other calculations work similarly (use graphical calculus as a tool for intuition).

Finally we have to check that $\Delta : R \rightarrow R \underline{\otimes} R$ and $\varepsilon : R \rightarrow k$ are algebra morphisms, where $R \underline{\otimes} R$ is an algebra with multiplication $(\mu \otimes \mu)(R \otimes \tau c \tau \otimes R)$. For ε this is clear. For Δ we have to check

$$\Delta^{cop} \mu^{op} = (\mu^{op} \otimes \mu^{op})(R \otimes \tau c \tau \otimes R)(\Delta^{cop} \otimes \Delta^{cop}).$$

As R is a braided bialgebra the left hand side is

$$\tau \Delta \mu \tau = \tau(\mu \otimes \mu)(R \otimes c \otimes R)(\Delta \otimes \Delta) \tau.$$

Now because Δ, μ commute with τ this is equal to

$$(\mu \otimes \mu)(R \otimes \tau \otimes R)(\tau \otimes \tau)(R \otimes \tau c \tau \otimes R)(\tau \otimes \tau)(R \otimes \tau \otimes R)(\Delta \otimes \Delta).$$

Thus it suffices to show

$$(R \otimes \tau \otimes R)(\tau \otimes \tau)(R \otimes \tau c \tau \otimes R)(\tau \otimes \tau)(R \otimes \tau \otimes R) = (\tau \otimes \tau)(R \otimes \tau c \tau \otimes R)(\tau \otimes \tau),$$

but this is trivial (check on elements). \square

Related material can be found in [22].

Assume now that (V, c) is a braided vector space. Denote the braided tensor bialgebra defined in section 2 by $(T(V, c), \mu, \eta, \Delta_c, \varepsilon, c)$. As an algebra this is $T(V)$.

Proposition 44 *Let (V, c) be a braided vector space. Let*

$$\phi : T(V, c) \rightarrow T(V, \tau c \tau)^{op, cop}$$

be the unique algebra morphism $T(V) \rightarrow T(V)^{op}$ given by $\phi|_V = \text{id}_V$. Then ϕ is an isomorphism of braided bialgebras.

For $v_1, \dots, v_n \in V$ we have

$$\phi(v_1 \otimes \dots \otimes v_n) = v_n \otimes \dots \otimes v_1.$$

PROOF. Lemma 6 gives us the existence of ϕ as a morphism of braided bialgebras because (V, c) is a braided subspace of $T(V, \tau c \tau)^{op, cop}$. By construction we see that ϕ is bijective and has the form given in the lemma. \square

Now we can prove the existence of the PBW basis in the right triangular case.

Theorem 45 *Assume (V, c) is a finite dimensional right triangular braided vectorspace and $I \subsetneq T(V, c)$ is a braided biideal. Then there is a totally ordered subset $S \subset T(V, c)$ and a height function $h : S \rightarrow \mathbb{N} \cup \{\infty\}$ such that the images of the PBW set generated by S and h form a basis of $T(V, c)/I$.*

Let

$$\phi : T(V, c) \rightarrow T(V, \tau c \tau)^{op, cop}$$

be the isomorphism from proposition 44. We have

$$S = \phi^{-1}(S_{\phi(I)}) \text{ and } h = h_{\phi(I)} \phi$$

and the order on the set S is the opposite of the order on $S_{\phi(I)}$.

PROOF. As $\phi(I)$ is a braided biideal in $T(V, \tau c \tau)^{op, cop}$ it is also a braided biideal in $T(V, \tau c \tau)$. As c is right triangular we have that $\tau c \tau$ is left triangular. So we find a set $S_{\phi(I)} \subset T(V, \tau c \tau)$ with a total ordering $<$ and a height function $h_{\phi(I)} : S \rightarrow \mathbb{N} \cup \{\infty\}$ such that the PBW set generated by these data in $T(V, \tau c \tau)$ is a basis for a complement of $\phi(I)$. The PBW set generated in $T(V, \tau c \tau)^{op, cop}$ by $S_{\phi(I)}$ with reversed order and height function $h_{\phi(I)}$ is the same set and thus also a basis for a complement of $\phi(I)$. The claim follows by transferring this set to $T(V, c)$ via ϕ^{-1} . \square

Together with the characterization of Nichols algebras given in [18] we obtain

Corollary 46 *Let (V, c) be a braided vectorspace. Then*

$$\mathcal{B}(V, \tau c \tau)^{op, cop} \simeq \mathcal{B}(V, c)$$

as braided graded Hopf algebras.

PROOF. In [18] the kernel of the canonical projection

$$\pi_c : T(V, c) \rightarrow \mathcal{B}(V, c)$$

is characterized as the sum over all coideals that are also homogenous ideals generated by elements of degree ≥ 2 . Using this we see that the map ϕ from proposition 44 maps $\ker \pi_c$ bijectively into $I := \ker \pi_{\tau c \tau} \subset T(V, \tau c \tau)$. As obviously

$$T(V, \tau c \tau)^{op, cop} / I = (T(V, \tau c \tau) / I)^{op, cop} \simeq \mathcal{B}(V, \tau c \tau)^{op, cop}$$

we get that ϕ induces the desired isomorphism of braided Hopf algebras. \square

8 Application to pointed Hopf algebras with abelian coradical

In this section we will show how to obtain a PBW basis for a Hopf algebra generated by an abelian group and a finite dimensional G -module spanned by skew primitive elements. On one hand this yields a generalization of the result in [1] as there the skew primitive elements are assumed to be semi-invariants (i.e. that the group acts on them by a character). On the other hand we lose some properties of the basis as already mentioned in remark 36.

Let $A = \cup_{n \geq 0} A_n$ be a filtered algebra. We can define a map

$$\pi : A \rightarrow \text{gr } A$$

by setting $\pi(0) := 0$ and for all $0 \neq a \in A : \pi(a) := a + A_{n-1}$ for the unique $n \geq 0$ such that $a \in A_n \setminus A_{n-1}$ (where $A_{-1} := \{0\}$ as usual). We will use this map to obtain PBW bases for A from homogenous PBW bases of the associated graded algebra $\text{gr } A$.

Proposition 47 *Let $A = \cup_{n \geq 0} A_n$ be a filtered algebra and $(P, S, <, h)$ a PBW basis for $\text{gr } A$ such that $P \subset \text{gr } A(0) = A_0$ and S is made up of homogenous elements. Then there is a PBW basis $(P, S', <', h')$ of A such that for all $a, b \in S'$*

$$\pi(a) \in S, h'(a) = h(\pi(a)) \text{ and } a < b \Leftrightarrow \pi(a) <' \pi(b).$$

PROOF. For all $s \in S \cap \text{gr } A(n)$ we find $\hat{s} \in A_n \setminus A_{n-1}$ such that $\pi(\hat{s}) = s$. Define

$$S' := \{\hat{s} | s \in S\}.$$

The map $S \rightarrow S', s \mapsto \hat{s}$ is bijective. So we can transfer the height function h and the order $<$ to S' obtaining h' and $<'$.

Assume we have $b := s_1^{e_1} \dots s_r^{e_r} p \in B(P, S, <, h)$. We define a lift

$$\hat{b} := \hat{s}_1^{e_1} \dots \hat{s}_r^{e_r} p \in B(P, S', <', h').$$

As the s_i and p are homogenous (say of degrees n_i and 0), also b is homogenous, say of degree n . Then

$$b = (\hat{s}_1 + A_{n_1-1})^{e_1} \dots (\hat{s}_r + A_{n_r-1})^{e_r} (p + A_{-1}) = \hat{s}_1^{e_1} \dots \hat{s}_r^{e_r} p + A_{n-1} = \hat{b} + A_{n-1}$$

in $\text{gr } A(n) = A_n / A_{n-1}$. We have $\hat{b} \in A_n \setminus A_{n-1}$, because otherwise ($\hat{b} \in A_{n-1}$) we had $b = 0$, but this is an element of a basis.

Let $B_n := B(P, S, <, h) \cap \text{gr } A(n)$ and $\hat{B}_n := \{\hat{b} | b \in B_n\}$. We will show by induction on $n \geq 0$ that $\hat{B}_0 \cup \dots \cup \hat{B}_n$ generates A_n as a vector space. The case $n = 0$ is trivial as $A_0 = \text{gr } A(0)$ has basis P . Assume $n \geq 0$ and $a \in A_n \setminus A_{n-1}$. We have $\pi(a) = a + A_{n-1} \in \text{gr } A(n)$ and thus $\pi(a)$ is a linear combination of elements of B_n i.e.

$$\pi(a) = a + A_{n-1} \in kB_n = \sum_{b \in B_n} k(\hat{b} + A_{n-1})$$

So we get that a is a linear combination of elements from \hat{B}_n and A_{n-1} and by induction assumption a is a linear combination of elements from $\hat{B}_0 \cup \dots \cup \hat{B}_n$.

We are left to show that $B(P, S', <', h')$ is linearly independent. Assume we have for all $b \in B_n$ scalars $\alpha_b \in k$ such that

$$\sum_{b \in B_n} \alpha_b \hat{b} \in A_{n-1}.$$

It suffices to show for all b that $\alpha_b = 0$. As we have seen above we have for all $b \in B(P, S, <, h) : b = \pi(\hat{b})$. Thus we have in $\text{gr } A(n)$:

$$\sum_{b \in B_n} \alpha_b b = \sum_{b \in B_n} \alpha_b (\hat{b} + A_{n-1}) = \left(\sum_{b \in B_n} \alpha_b \hat{b} \right) + A_{n-1} = 0$$

As B_n is a linearly independent we obtain for all $b \in B_n \setminus B_{n-1} : \alpha_b = 0$. \square

Theorem 48 *Let k be an algebraically closed field. Let H be a Hopf algebra generated by an abelian group G and skew primitive elements a_1, \dots, a_t such that the subvectorspace of H spanned by a_1, \dots, a_t is stable under the adjoint action of G . Then H has a PBW basis $(G, S, <, h)$.*

PROOF. First we may assume that for all $1 \leq i \leq t$

$$\Delta(a_i) = g_i \otimes a_i + a_i \otimes 1.$$

Let H_n be the subspace of H generated by all products of elements of G and at most n factors from $\{a_1, \dots, a_t\}$. This defines a Hopf algebra filtration of H . It is well known from [18,23,24] that we can decompose the associated graded Hopf algebra

$$\text{gr } H \simeq R \# kG,$$

as graded Hopf algebras, where R is a braided graded Hopf algebra in ${}^{kG}_k \mathcal{YD}$ generated by the finite dimensional Yetter-Drinfel'd submodule $R(1) \subset P(R)$. As a G module $R(1)$ is isomorphic to $ka_1 + \dots + ka_t$ with the adjoint G -action.

Example 19 shows that the braiding on $R(1)$ is triangular because the group G is abelian. So by the PBW theorem 35 we find a PBW basis $(\{1\}, S, <, h)$ of R . This implies that $(1 \# G, S \# 1, <, h)$ is a PBW basis of $\text{gr } H$ and thus we find a PBW basis of H using the proposition above. \square

9 Examples

Finally we will deal with some interesting examples mentioned in [13] that are not of diagonal type by remark 21, namely the Nichols algebras of simple $U_q(\mathfrak{sl}_2)$ modules of low dimension (and type +1). Let $q \in \mathbb{C}$ be not a root of unity and $(M, c) = L(n, +1)$ be the simple $U_q(\mathfrak{sl}_2)$ module of dimension $n+1$ and type +1. Denote its natural basis (see e.g. [20]) by x_0, \dots, x_n and order this basis by $x_0 < \dots < x_n$. Then the braidings from example 18 are left (and right) triangular with respect to this basis. For calculations we assume for the map f that $f(\frac{\alpha}{2}, \frac{\alpha}{2}) = q^{-2} = f(0, 0)$ (see [20, chapters 3 and 7]).

- (1) $n = 1$: As for example shown in [18], $\mathcal{B}(M, c)$ is a quadratic algebra. The relation in degree two is

$$x_0x_1 - qx_1x_0 = 0.$$

Thus the set of PBW generators S contains only Lyndon words in x_0, x_1 that do not have x_0x_1 as a subword. This means $S = \{x_0, x_1\}$. As the diagonal coefficients of c are powers of q by lemma 42 all elements have infinite height. Thus the elements of the form $x_1^i x_0^j, i, j \in \mathbb{N}_0$ form a basis for $\mathcal{B}(M, c)$.

- (2) $n = 2$: Here we have the following relations in degree two:

$$\begin{aligned} x_0x_1 - q^2x_1x_0 &= 0, \\ x_1x_2 - q^2x_2x_1 &= 0, \\ x_0x_2 + (q^2 - 1)x_1x_1 - x_2x_0 &= 0. \end{aligned}$$

So all words in S are Lyndon words in x_0, x_1, x_2 that do not contain one of x_0x_1, x_1x_2, x_0x_2 as a subword. As surely $x_0, x_1, x_2 \in S$ this leaves $S = \{x_0, x_1, x_2\}$. Again by lemma 42 all elements of S have infinite height and thus the elements of the form $x_2^i x_1^j x_0^k, i, j, k \in \mathbb{N}_0$ form a basis of $\mathcal{B}(M, c)$. In particular this is a quadratic algebra.

- (3) $n = 3$: In this case the space of relations of degree two can be calculated using Maple. It is generated by the relations

$$\begin{aligned} x_0x_1 - q^3x_1x_0 &= 0, \\ x_0x_2 + \frac{1 - q^4}{q}x_1^2 - x_2x_0 &= 0, \\ q^3x_0x_3 + q^2(q^2 + 1 - q^4)x_1x_2 + (q - q^3 - q^5)x_2x_1 - x_3x_0 &= 0, \\ x_1x_3 + \frac{1 - q^6}{q(q^2 + 1)}x_2^2 - x_3x_1 &= 0, \\ x_2x_3 - q^3x_3x_2 &= 0. \end{aligned}$$

By combining these relations one obtains the additional relations

$$\begin{aligned} (q^4 - q^2 + 1)x_1x_2x_2 - q(q^6 + 1)x_2x_1x_2 + (q^4 - q^2 + 1)q^4x_2x_2x_1 &= 0, \\ x_1x_1x_2 - q(q^2 + 1)x_1x_2x_1 + q^4x_2x_1x_1 &= 0. \end{aligned}$$

As q is a root of unity, the leading coefficients in these relations are not zero: the zeros of $X^4 - X^2 + 1$ are primitive 12-th roots of unity as

$$X^{12} - 1 = (X^4 - X^2 + 1)(X^2 + 1)(1 - X^6).$$

Thus S can only contain Lyndon words in x_0, x_1, x_2, x_3 that do not contain a subword from the following list:

$$x_0x_1, x_0x_2, x_0x_3, x_1x_3, x_2x_3, x_1^2x_2, x_1x_2^2.$$

It follows that $S \subset \{x_0, x_1, x_2, x_3, x_1x_2\}$. None of these words can be expressed by standard-bigger ones as we can see from the relations of degree 2. Thus $S = \{x_0, x_1, x_2, x_3, x_1x_2\}$ and the elements of the form $x_3^ax_2^b(x_1x_2)^cx_1^dx_0^e, a, b, c, d, e \in \mathbb{N}_0$ form a basis of $\mathcal{B}(M, c)$. In particular $\mathcal{B}(M, c)$ is a quadratic algebra.

References

- [1] V. Kharchenko, A quantum Analog of the Poincaré-Birkhoff-Witt Theorem, *Algebra and Logic* Vol. 38 (4) (1999) 259–276.
- [2] C. Reutenauer, *Free Lie Algebras*, Vol. 7 of London Mathematical Society Monographs, New Series, Clarendon Press, London, 1993.
- [3] P. Lalonde, A. Ram, Standard Lyndon bases of Lie algebras and enveloping algebras, *Trans. Amer. Math. Soc.* 347 (5) (1995) 1821–1830.
- [4] G. Lusztig, Finite-dimensional Hopf algebras arising from quantized enveloping algebras, *J. Amer. Math. Soc.* 3 (1) (1990) 257–296.
- [5] G. Lusztig, Introduction to quantum groups, no. 110 in *Progress in Mathematics*, Birkhäuser, 1993.
- [6] M. Rosso, An analogue of the PBW theorem and the universal R -matrix for $U_hsl(N+1)$, *Comm. Math. Phys.* 124 (2) (1989) 307–318.
- [7] M. Rosso, Quantum Groups and quantum Shuffles, *Inventiones Math.* 133 (1998) 399–416.
- [8] C. Ringel, PBW-bases of quantum groups, *J. reine angewandte Mathematik* 470 (1990) 51–88.
- [9] V. Drinfel'd, Hopf algebras and the quantum Yang-Baxter equation, *Dokl. Akad. Nauk SSSR* 283:5 (1985) 1060–1064.
- [10] V. Drinfel'd, Quantum groups, in: *Proc. Int. Cong. Math. (Berkeley 1986)*, Amer. Math. Soc., Providence, RI, 1987, pp. 798–820.
- [11] M. Jimbo, A q -differences analogue of $U(\mathfrak{g})$ and the Yang-Baxter equation, *Lett. Math. Phys.* 10 (1985) 63–69.
- [12] B. Leclerc, Dual canonical Bases, quantum Shuffles and q -Characters, preprint at arXiv:math.QA/0209133v1, to appear in *Math. Zeitschrift*.
- [13] N. Andruskiewitsch, Some Remarks on Nichols Algebras, preprint at arXiv:math.QA/0301064.
- [14] M. Lothaire, *Combinatorics on Words*, Vol. 17 of *Encyclopedia of Mathematics and its Applications*, Addison-Wesley, 1983.

- [15] V. Ufnarovski, Combinatorial and asymptotic Methods in Algebra, in: Kostrikin, Shafarevich (Eds.), Algebra VI, no. 57 in Encyclopaedia of Mathematical Sciences, Springer, 1994.
- [16] M. Takeuchi, Survey of braided Hopf Algebras, in: New trends in Hopf Algebra Theory, no. 267 in Contemporary Mathematics, 1999, pp. 301–323.
- [17] P. Schauenburg, A Characterization of the Borel-like Subalgebras of quantum enveloping Algebras, Comm. in Algebra 24 (1996) 2811–2823.
- [18] N. Andruskiewitsch, H.-J. Schneider, Pointed Hopf Algebras, in: New directions in Hopf algebras, Vol. 43 of MSRI Publications, Cambridge University Press, 2002, pp. 1–68.
- [19] S. Ufer, Braidings and pointed Hopf algebras, preprint 2003.
- [20] J. Jantzen, Lectures on quantum Groups, Vol. 6 of Graduate Studies in Mathematics, Am. Math. Soc., 1995.
- [21] V. Kharchenko, A combinatorial Approach to the Quantification of Lie Algebras, Pacific J. Math. 203 (1) (2002) 191–233.
- [22] N. Andruskiewitsch, M. Graña, Braided Hopf algebras over non-abelian Groups, Bol. Acad. Ciencias (Cordoba) 63 (1999) 45–78.
- [23] D.E. Radford, Hopf algebras with projection, J. Algebra 92 (1985) 322–347.
- [24] S. Majid, Crossed products by braided groups and bosonization, J. Algebra 163 (1994) 165–190.
- [25] J. Humphreys, Reflection Groups and Coxeter Groups, Vol. 29 of Cambridge studies in advanced mathematics, Cambridge University Press, 1994.